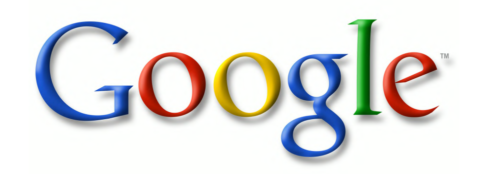


This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

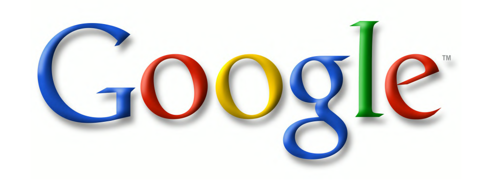
+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at http://books.google.com/



Это цифровая коиия книги, хранящейся для иотомков на библиотечных иолках, ирежде чем ее отсканировали сотрудники комиании Google в рамках ироекта, цель которого - сделать книги со всего мира достуиными через Интернет.

Прошло достаточно много времени для того, чтобы срок действия авторских ирав на эту книгу истек, и она иерешла в свободный достуи. Книга иереходит в свободный достуи, если на нее не были иоданы авторские ирава или срок действия авторских ирав истек. Переход книги в свободный достуи в разных странах осуществляется ио-разному. Книги, иерешедшие в свободный достуи, это наш ключ к ирошлому, к богатствам истории и культуры, а также к знаниям, которые часто трудно найти.

В этом файле сохранятся все иометки, иримечания и другие заииси, существующие в оригинальном издании, как наиоминание о том долгом иути, который книга ирошла от издателя до библиотеки и в конечном итоге до Вас.

Правила использовапия

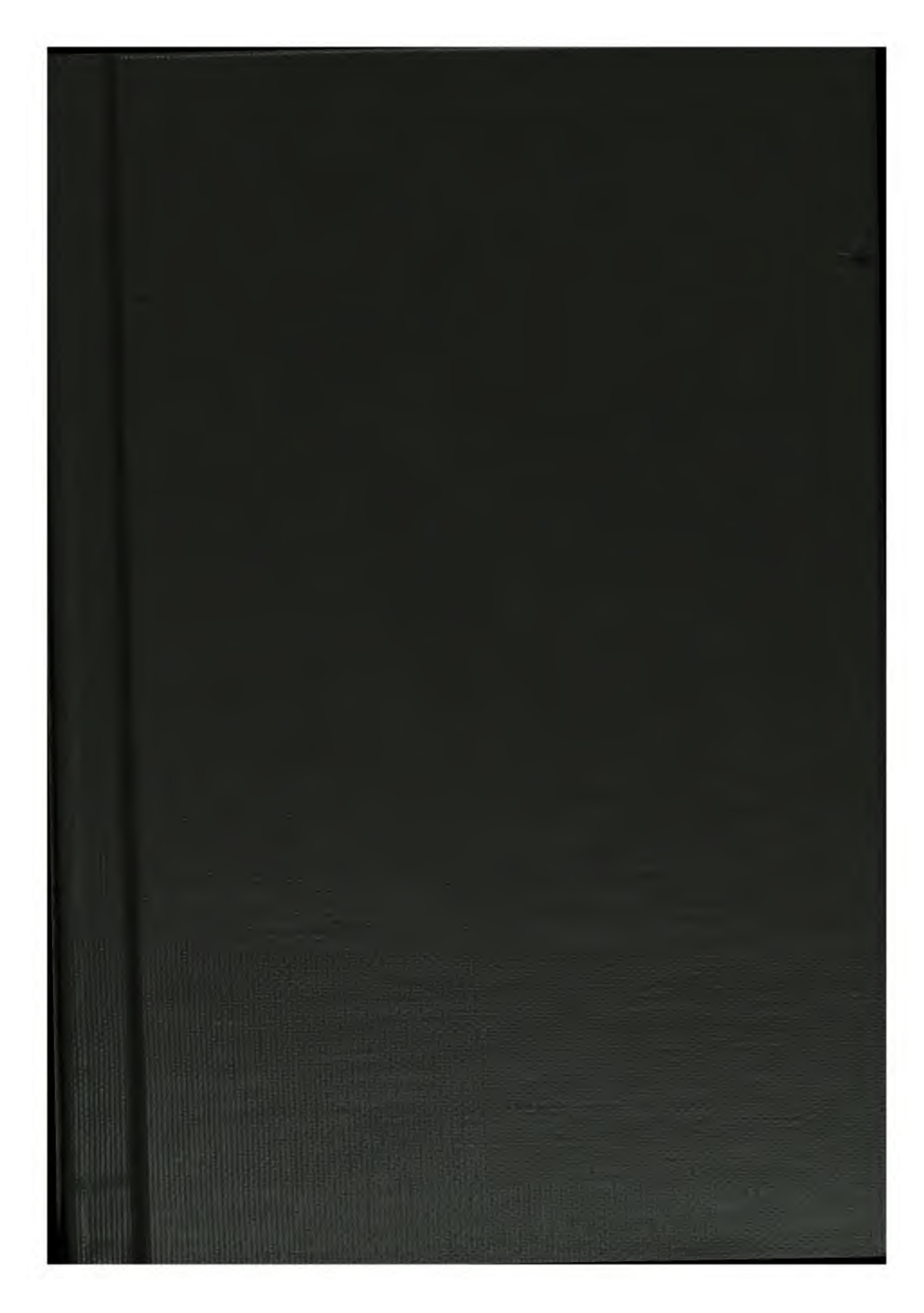
Комиания Google гордится тем, что сотрудничает с библиотеками, чтобы иеревести книги, иерешедшие в свободный достуи, в цифровой формат и сделать их широкодостуиными. Книги, иерешедшие в свободный достуи, ирипадлежат обществу, а мы лишь хранители этого достояния. Тем не менее, эти книги достаточно дорого стоят, иоэтому, чтобы и в дальнейшем иредоставлять этот ресурс, мы иредириняли некоторые действия, иредотвращающие коммерческое исиользование книг, в том числе установив технические ограничения на автоматические заиросы.

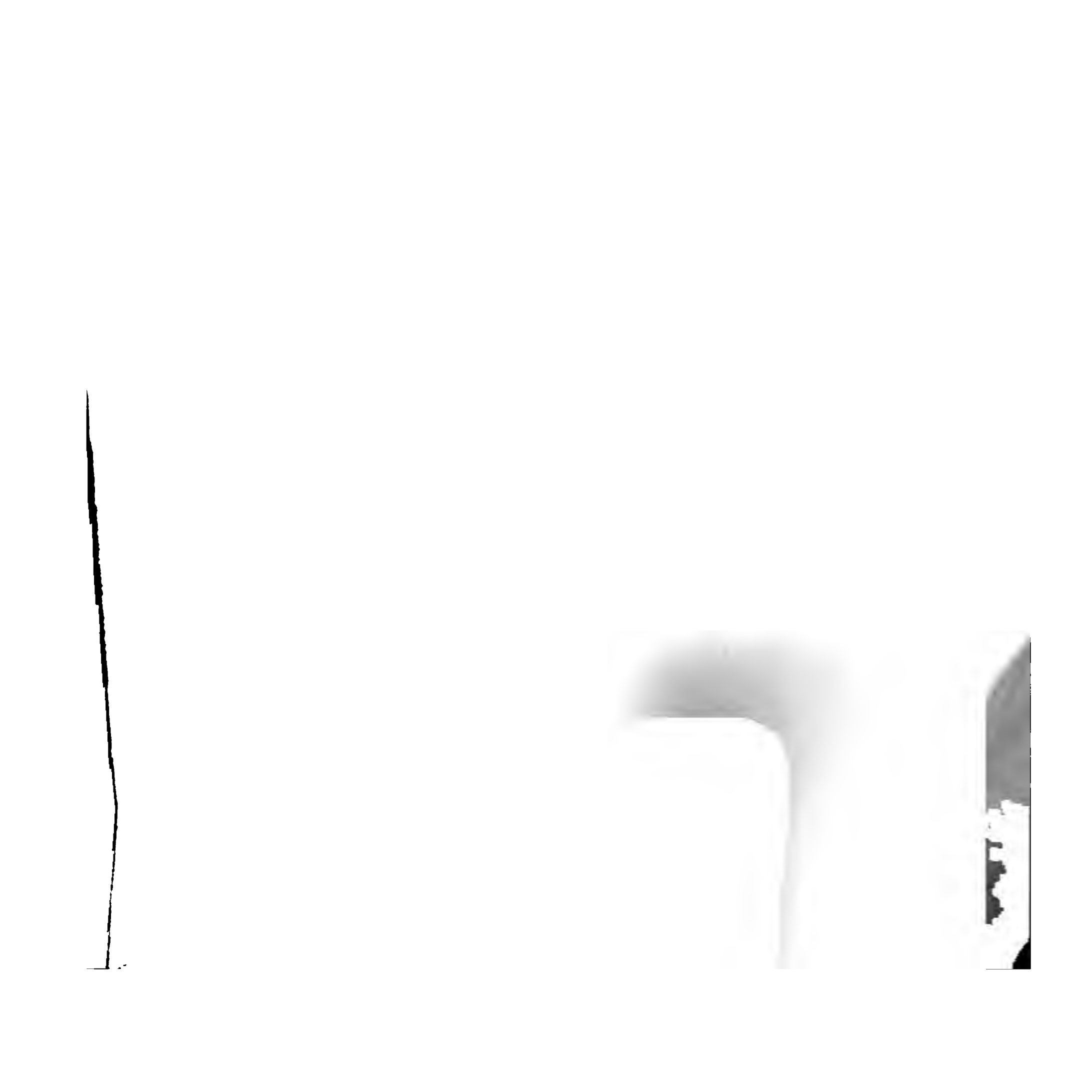
Мы также иросим Вас о следующем.

- Не исиользуйте файлы в коммерческих целях.
  Мы разработали ирограмму Поиск книг Google для всех иользователей, иоэтому исиользуйте эти файлы только в личных, некоммерческих целях.
- Не отиравляйте автоматические заиросы.
  Не отиравляйте в систему Google автоматические заиросы любого вида. Если Вы занимаетесь изучением систем машинного иеревода, оитического расиознавания символов или других областей, где достуи к большому количеству текста может оказаться иолезным, свяжитесь с нами. Для этих целей мы рекомендуем исиользовать материалы, иерешедшие в свободный достуи.
- Не удаляйте атрибуты Google.
  В каждом файле есть "водяной знак" Google. Он иозволяет иользователям узнать об этом ироекте и иомогает им найти доиолнительные материалы ири иомощи ирограммы Поиск книг Google. Не удаляйте его.
- Делайте это законно.
  Независимо от того, что Вы исиользуйте, не забудьте ироверить законность своих действий, за которые Вы несете иолную ответственность. Не думайте, что если книга иерешла в свободный достуи в США, то ее на этом основании могут исиользовать читатели из других стран. Условия для иерехода книги в свободный достуи в разных странах различны, иоэтому нет единых иравил, иозволяющих оиределить, можно ли в оиределенном случае исиользовать оиределенную книгу. Не думайте, что если книга иоявилась в Поиске книг Google, то ее можно исиользовать как угодно и где угодно. Наказание за нарушение авторских ирав может быть очень серьезным.

О программе Поиск кпиг Google

Миссия Google состоит в том, чтобы организовать мировую информацию и сделать ее всесторонне достуиной и иолезной. Программа Поиск книг Google иомогает иользователям найти книги со всего мира, а авторам и издателям - новых читателей. Полнотекстовый иоиск ио этой книге можно выиолнить на странице http://books.google.com/





QA 155 .S65 1882 C.1
Vysshaia algebra /
Stanford University Libraries
3 6105 034 783 907

DATE DUE		

STANFORD UNIVERSITY LI
STANFORD, CALIFORNIA

Gift of

Joseph J. Smortchevsky

LELAND STANFORD JUNIOR UNIVERSITY
ORGANIZED 1891

STANFORD UNIVERSITY LIBRARIES





Sokhotskii, I.V.

ВЫСШАЯ АЛГЕБРА.

ЧАСТЬ ВТОРАЯ,

НАЧАЛА ТЕОРІИ ЧИСЕЛЪ.

Ю. СОХОЦКАГО.

САНКТПЕТЕРБУРГЪ.
ТИПОГРАФІЯ ИМПЕРАТОРСКОЙ АКАДЕМІИ НАУКЪ.
Вас. Остр., 9 лин., № 12.
1888.

From the books of
Joseph J. Smortchevsky
Vancouver, B.C., Canada, 1986

ПРЕДИСЛОВІЕ.

Въ алгебраическихъ изысканіяхъ важную роль играютъ индивидуальныя свойства степени уравненія: приходится часто говорить одно объ уравненіяхъ простой степени, другое — объ уравненіяхъ сложной степени; дальнѣйшія различія въ характерѣ степени вызываютъ новыя различія въ пріемахъ и въ окончательныхъ выводахъ. Съ другой стороны, самыя общія, первоначальныя изысканія надъ корнями уравненія указываютъ на необходимость предварительной разработки теоріи перестановокъ, — науки спеціальной, заимствующей многое существенное изъ теоріи чиселъ. Потому-то, прежде чѣмъ приступить къ общей теоріи алгебраическихъ уравненій, необходимо познакомиться съ основными свойствами цѣлыхъ чиселъ, и хорошо усвоить себѣ разнообразные пріемы, употребляемые въ теоріи послѣднихъ.

Но связь алгебры съ теоріею чиселъ болѣе тѣсна, чѣмъ можно заключить на основаніи вышесказаннаго.

Примѣненіе способовъ, предлагаемыхъ въ алгебрѣ для рѣшенія разныхъ вопросовъ, ставитъ на видъ различіе между буквенными уравненіями и числовыми; и понятно, что послѣднія должны представлять большій интересъ, чѣмъ первыя.

Между числовыми уравненіями первое мѣсто принадлежитъ уравненіямъ съ цѣлыми коеффиціентами. Корни такихъ уравненій составляютъ новый ариѳметическій алгориѳмъ; переходъ къ нимъ отъ цѣлыхъ чиселъ представляется столь же естественнымъ, какъ въ геометріи переходъ отъ прямой линіи къ кривымъ. И подобно тому, какъ въ геометріи разсматриваніе кривыхъ второй степени привело къ самымъ драгоцѣннымъ послѣдствіямъ, точно также и въ алгебрѣ изслѣдованіе цѣлыхъ алгебраическихъ чиселъ втораго порядка приводитъ къ постановкѣ новыхъ вопросовъ и къ рѣшенію новыхъ задачъ, представляющихъ высшій научный интересъ. Благодаря этому теорія чиселъ поставлена на ступень тѣхъ немногихъ наукъ, которыя особенно выдаются по точности, простотѣ и изяществу своихъ пріемовъ.

Здѣсь, конечно, я не имѣю въ виду особенныхъ вопросовъ теоріи чиселъ, рѣшеніе которыхъ, кажется, превосходитъ силы современнаго конечнаго анализа.

Существуетъ немного примѣровъ своеобразнаго и чрезвычайно удачнаго примѣненія трансцендентнаго анализа къ рѣшенію нѣкоторыхъ изъ означенныхъ вопросовъ; подобныя работы, хотя и относятся къ теоріи чиселъ, но составляютъ совершенно отдѣльную ея вѣтвь, выходящую изъ области конечнаго анализа.

Современная теорія чиселъ построена на трехъ началахъ: 1° общій наибольшій дѣлитель (Евклидъ), 2° непрерывныя дроби (Гюгенсъ), 3° начало Дирихле. Настоящая книга посвящена исключительно началу Евклида въ приложеніи къ цѣлымъ числамъ и цѣлымъ функціямъ; потому можно было бы ее озаглавить: „теорія дѣлимости“ или „теорія сравненій“.

Особенное вниманіе было обращено мною на тѣ мѣста, которыя находятъ приложеніе въ дальнѣйшихъ частяхъ алгебры. Такъ, напримѣръ, линейныя сравненія со многими неизвѣстными играютъ существенную роль въ теоріи подстановокъ; потому я останавливаюсь на нихъ немного дольше, чѣмъ Гауссъ въ его „Disquisitiones arithmeticae“.

Въ концѣ первой главы я показываю способы рѣшенія въ цѣлыхъ числахъ нѣсколькихъ неопредѣленныхъ уравненій первой степени, которыя могутъ показаться не особенно важными; между тѣмъ въ нихъ содержится рѣшеніе вопроса объ умноженіи такъ называемыхъ идеальныхъ чиселъ (втораго порядка) или, все

равно, о сложеніи квадратичныхъ формъ (Gauss, compositio formarum), — одинъ изъ самыхъ плодотворныхъ вопросовъ въ теоріи чиселъ.

Въ общемъ, книга эта представляетъ развитіе моихъ университетскихъ лекцій, на сколько таковое необходимо для основательнаго уразумѣнія высшихъ вопросовъ современной алгебры.

ОГЛАВЛЕНІЕ.

ГЛАВА I.

Начало общаго наибольшаго дѣлителя. — Первыя приложенія.

§ I. Начало общаго наибольшаго дѣлителя.

§ II. Разложеніе чиселъ на простые множители.

§ III. Условія дѣлимости. Слѣдствія.

ГЛАВА II.

Рѣшеніе въ цѣлыхъ числахъ нѣсколькихъ неопредѣленныхъ задачъ.

§ I. Общее рѣшеніе линейнаго однороднаго уравненія.

§ II. Составленіе опредѣлителя, значеніе котораго равно 1, при данныхъ элементахъ первой строки.

§ III. Составленіе опредѣлителя при другихъ условіяхъ.

§ IV. Новое рѣшеніе предыдущей задачи въ частномъ случаѣ, когда опредѣлитель 4-го порядка.

ГЛАВА III.

Понятіе о сравненіяхъ. — Сравненія первой степени.

§ I. О сравненіяхъ вообще.

§ II. О наименьшихъ вычетахъ.

§ III. Теорема Фермата.

§ IV. Слѣдствія изъ теоремы Ферма.

§ V. Рѣшеніе сравненій первой степени.

§ VI. Рѣшеніе совокупныхъ сравненій съ нѣсколькими неизвѣстными.

ГЛАВА IV.

Сравненія 2-ой степени. — Законъ взаимности простыхъ чиселъ.

§ I. Приведеніе сравненія къ простѣйшему виду. Условіе рѣшимости при модулѣ простомъ.

§ II. Символъ Лежандра.

§ III. Символъ Якоби.

§ IV. Рѣшеніе сравненія второй степени въ двухъ частныхъ случаяхъ.

ГЛАВА V.

Квадратичные вычеты и невычеты. — О дѣлителяхъ формы $t^2 - Du^2$.

§ I. О квадратичныхъ вычетахъ.

§ II. О рѣшеніяхъ уравненія $\left(\frac{D}{x}\right) = \pm 1$.

ГЛАВА VI.

Сравненіе второй степени при сложномъ модулѣ.

§ I. Случай, когда модуль есть степень простаго числа.

§ II. Число рѣшеній сравненія второй степени при сложномъ модулѣ. Слѣдствія.

ГЛАВА VII.

О сравненіяхъ высшихъ степеней. — Двучленныя сравненія.

§ I. Теорема Лагранжа.

§ II. Разложеніе функцій на множители по данному модулю.

§ III. Пониженіе степени сравненія.

§ IV. О двучленныхъ сравненіяхъ.

ГЛАВА VIII.

Теорія первообразныхъ корней. — Свойства индексовъ.

§ I. О показателяхъ чиселъ по данному модулю.

§ II. О первообразныхъ корняхъ простыхъ чиселъ.

§ III. О первообразныхъ корняхъ чиселъ вида p^m или $2p^m$.

§ IV. Опредѣленіе наибольшаго показателя при какомъ угодно модулѣ.

§ V. Обобщеніе теоремы Вильсона.

§ VI. Теорія индексовъ.

ГЛАВА IX.

О функціональныхъ сравненіяхъ и неприводимыхъ функціяхъ.

§ I. Сравненія съ двойнымъ модулемъ.

§ II. Теорема Лагранжа.

§ III. Разложеніе функціи $x^{p^n} - x$ на неприводимые множители по модулю p.

§ IV. О показателяхъ функцій по данному модулю.

§ V. О надпоказателяхъ функцій по данному модулю.

§ VI. Число функцій, принадлежащихъ къ данному надпоказателю.

§ VII. О порядкахъ неприводимыхъ функцій.

ГЛАВА X.

О функціяхъ абсолютно неприводимыхъ.

§ I. Начала дѣлимости.

§ II. Доказательство одного сравненія.

§ III. Разложеніе функціи x^m-1 на неприводимые множители.

§ IV. Новое доказательство неприводимости функцiи ψ_m при m равномъ степени простаго числа.

НАЧАЛА ТЕОРІИ ЧИСЕЛЪ.

ГЛАВА I.

Начало общаго наибольшаго дѣлителя. — Первыя приложенія. — Разложеніе чиселъ на простые множители и условія дѣлимости. — Свойства функціи $\varphi(a)$. — Разныя приложенія предыдущаго.

§ I. Начало общаго наибольшаго дѣлителя.

1. Пусть будутъ два цѣлыхъ положительныхъ числа a и b, изъ коихъ a не меньше b. Произведемъ рядъ послѣдовательныхъ дѣленій въ слѣдующемъ порядкѣ: раздѣлимъ a на b, частное обозначимъ чрезъ p_1, остатокъ чрезъ d_1; затѣмъ раздѣлимъ b на d_1, частное обозначимъ чрезъ p_2, остатокъ чрезъ d_2; раздѣлимъ, далѣе, d_1 на d_2, частное обозначимъ чрезъ p_3, остатокъ чрезъ d_3, — и будемъ продолжать дѣйствовать такимъ образомъ до тѣхъ поръ, пока не дойдемъ до остатка равнаго нулю; это произойдетъ неминуемо, ибо числа d_1, d_2, d_3, . . . идутъ убывая, и не могутъ сдѣлаться отрицательными. Положивъ, что послѣдній остатокъ не равный нулю есть d_n, будемъ имѣть рядъ уравненій

$$a = bp_1 + d_1,$$

$$b = d_1p_2 + d_2,$$

$$d_1 = d_2 p_3 + d_3,$$

. . . .

. . . .

$$d_{n-3} = d_{n-2} p_{n-1} + d_{n-1},$$

$$d_{n-2} = d_{n-1} p_n + d_n,$$

$$d_{n-1} = d_n p_{n+1}.$$

Отсюда выводимъ

$$d_{n-2} = (p_n p_{n+1} + 1) d_n = u_{n-2} d_n,$$

$$d_{n-3} = (p_{n-1} u_{n-2} + p_{n+1}) d_n = u_{n-3} d_n,$$

$$d_{n-4} = (p_{n-2} u_{n-3} + u_{n-2}) d_n = u_{n-4} d_n,$$

. . . .

. . . .

$$b = (p_2 u_1 + u_2) d_n = u d_n,$$

$$a = (p_1 u + u_1) d_n = v d_n,$$

гдѣ $u_{n-2}, u_{n-1}, \ldots u, v$ изображаютъ извѣстныя цѣлыя числа.

Изъ предыдущихъ уравненій, производя исключенія въ другомъ порядкѣ, получаемъ рядъ новыхъ соотношеній, а именно:

$$d_1 = a - p_1 b,$$

$$d_2 = -p_2 a + (p_1 p_2 + 1) b = x_2 a + y_2 b,$$

$$d_3 = (1 - p_3 x_2) a - (p_1 + p_3 y_2) b = x_3 a + y_3 b,$$

. . . .

$d_{n-2} =$ . . . . $= x_{n-2} a + y_{n-2} b$

$d_{n-1} =$ $= x_{n-1} a + y_{n-1} b$

$$d_n = (x_{n-2} - p_n x_{n-1}) a + (y_{n-2} - p_n y_{n-1}) b = x_n a + y_n b,$$

гдѣ $x_2, x_3, \ldots y_2, y_3, \ldots$ изображаютъ извѣстныя цѣлыя числа.

Между уравненіями двухъ предыдущихъ группъ особенно важны три слѣдующія:

$$a = vd_n, \qquad b = ud_n, \qquad x_n a + y_n b = d_n.$$

Для сокращенія отбросимъ значки у буквъ x, y, d и напишемъ ихъ такъ:

$$(1) \; \ldots\ldots \; a = vd, \qquad b = ud, \qquad ax + by = d.$$

Послѣднее изъ этихъ уравненій показываетъ, что всякій общій дѣлитель чиселъ a и b дѣлитъ число d; а первыя два показываютъ обратное: что всякій дѣлитель числа d дѣлитъ оба числа a и b. Слѣдовательно вопросъ объ опредѣленіи общихъ дѣлителей какихъ либо двухъ данныхъ чиселъ a и b приводится вышеуказаннымъ образомъ къ опредѣленію всѣхъ дѣлителей числа d.

$a=qr$; $b=qt$; $ax+by = q(rx+ty) = d$; d дѣлится на q.

Число d есть *наибольшій общій дѣлитель* чиселъ a и b, потому что наибольшій дѣлитель числа d есть самое число d. Характеристическое свойство этого дѣлителя состоитъ въ слѣдующемъ.

Теорема. *Общій наибольшій дѣлитель d двухъ чиселъ a и b выражается посредствомъ этихъ чиселъ линейнымъ образомъ*

$$d = ax + by,$$

при цѣлыхъ значеніяхъ x и y, подобранныхъ надлежащимъ образомъ.

Справедливость этой теоремы показываетъ послѣднее изъ уравненій (1).

Слѣдствіе. *Наименьшая числовая величина линейной формы $ax + by$ при цѣлыхъ перемѣнныхъ x и y, какъ положительныхъ такъ и отрицательныхъ, равна общему наибольшему дѣлителю чиселъ a и b.* x)

Само собою разумѣется, что здѣсь рѣчь идетъ о значеніяхъ формы отличныхъ отъ нуля.

x) ибо большія числовыя величины формы, состоящія необходимо изъ общихъ дѣлителей a и b, могутъ быть только кратными общаго наибольшаго дѣлителя d.

Случай нѣсколькихъ чиселъ.

2. Чтобы найти общій наибольшій дѣлитель трехъ чиселъ a, b, c, слѣдуетъ опредѣлить сперва общій наибольшій дѣлитель d' чиселъ a и b, а затѣмъ общій наибольшій дѣлитель d чиселъ d' и c; этотъ послѣдній будетъ числомъ искомымъ, и всякій общій дѣлитель чиселъ a, b, c будетъ дѣлителемъ числа d.

При нѣкоторыхъ цѣлыхъ числахъ x', y', x'', y'' будутъ имѣть мѣсто два уравненія

$$ax' + by' = d',$$

$$d'x'' + cy'' = d;$$

отсюда, исключая d', получаемъ

$$ax'x'' + bx''y' + cy'' = d,$$

или, проще,

$$ax + by + cz = d,$$

гдѣ x, y, z изображаютъ извѣстныя цѣлыя числа. Слѣдовательно общій наибольшій дѣлитель трехъ чиселъ a, b, c выражается линейной однородной формой $ax + by + cz$ при нѣкоторыхъ цѣлыхъ значеніяхъ перемѣнныхъ x, y, z.

Сказаннаго достаточно, чтобы понять, какимъ образомъ, путемъ послѣдовательныхъ дѣленій, составляется общій наибольшій дѣлитель d какого угодно числа данныхъ чиселъ a, b, $c, \ldots l$, и что дѣлитель этотъ можно выразить линейною формой

$$d = ax + by + cz + \ldots + lt$$

при нѣкоторыхъ цѣлыхъ значеніяхъ перемѣнныхъ $x, y, z, \ldots t$.

Понятіе о числахъ взаимно простыхъ.

3. Два цѣлыхъ числа a и b называются *относительно простыми*, когда они, кромѣ единицы, не имѣютъ общаго дѣлителя, или, иначе, когда ихъ общій наибольшій дѣлитель равенъ единицѣ. Для этого необходимо и достаточно, чтобы неопредѣленное уравненіе

$$(1) \ldots\ldots\ldots\ldots \quad ax + by = 1$$

допускало рѣшеніе въ цѣлыхъ числахъ. Иногда приходится выражать то же самое предложеніе въ обратномъ порядкѣ: чтобы уравненіе (1) имѣло рѣшеніе въ цѣлыхъ числахъ, необходимо и достаточно, чтобы числа a и b были относительно простыми.

4. На основаніи вышеизложеннаго не трудно убѣдиться въ справедливости нижеслѣдующихъ двухъ теоремъ, выражающихъ основныя свойства относительно простыхъ чиселъ.

Свойства чисел взаимно простых.

Теорема 1. *Произведеніе двухъ чиселъ, простыхъ относительно третьяго, есть также простое относительно третьяго.*

Пусть будутъ два числа a и b, изъ коихъ каждое есть простое относительно третьяго числа c, и пусть x', x'', y', y'' изображаютъ цѣлыя числа, удовлетворяющія уравненіямъ

$$ax' + cy' = 1,$$

$$bx'' + cy'' = 1.$$

Намъ извѣстно, какъ находятся такія числа, и потому мы на нихъ будемъ смотрѣть, какъ на извѣстныя.

Напишемъ послѣднія равенства такъ:

$$ax' = 1 - cy',$$

$$bx'' = 1 - cy'',$$

и перемножимъ ихъ почленно; получаемъ

$$abx'x'' = 1 - c(y' + y'' - cy'y'').$$

Отсюда, полагая для сокращенія

$$x = x'x'',$$

$$y = y' + y'' - cy'y'',$$

выводимъ

$$abx + cy = 1.$$

Такъ какъ x и y суть очевидно числа цѣлыя, то изъ послѣдняго равенства слѣдуетъ, что ab и c суть числа относительно простыя. Что и слѣдовало доказать.

Слѣдствіе. *Если каждое изъ чиселъ* a, a_1, a_2, . . . *есть простое относительно каждаго изъ чиселъ* b, b_1, b_2, . . . , *то произведенія* $a\ a_1\ a_2$ . . . *и* $b\ b_1\ b_2$ . . . *суть взаимно простыя.*

Теорема 2. *Если* c, *будучи простымъ числомъ относительно* a, *дѣлитъ произведеніе* ab, *то оно дѣлитъ* b.

Дѣйствительно, такъ какъ a и c числа относительно простыя, то уравненіе

$$ax + cy = 1$$

имѣетъ рѣшеніе въ цѣлыхъ числахъ. Разсматривая x и y какъ извѣстныя, положимъ еще

$$ab = cz,$$

гдѣ z, по предположенію, число цѣлое. Исключая a изъ предыдущихъ уравненій, получаемъ

$$xz + by = \frac{b}{c}.$$

Здѣсь первая часть есть очевидно цѣлое число, слѣдовательно b дѣлится на c.

Слѣдствіе 1. *Если каждое изъ двухъ взаимно простыхъ чиселъ* a *и* b *дѣлитъ* c, *то и произведеніе* ab *дѣлитъ* c.

Дѣйствительно, полагая $c = aa'$, мы замѣчаемъ на основаніи послѣдней теоремы, что число a' дѣлится на b; полагая слѣдовательно $a' = ba''$, имѣемъ $c = aba''$. Это показываетъ, что c дѣлится на ab.

Имѣя нѣсколько чиселъ a, b, c, . . . k, мы будемъ называть ихъ *простыми между собою*, если каждыя два, произвольно взятыя между ними, будутъ относительно простыми. Общій наибольшій дѣлитель такой системы чиселъ очевидно равенъ еди-

ницѣ; но обратнаго нельзя утверждать. Такъ, напримѣръ, общій наибольшій дѣлитель чиселъ 4, 5, 6 равенъ 1, между тѣмъ они не простыя между собою.

Принимая это въ соображеніе, можно расширить послѣднее слѣдствіе, и выразить его въ слѣдующей формѣ.

Слѣдствіе 2. *Если числа a, b, c,...k простыя между собою, и каждое изъ нихъ дѣлитъ число l, то и произведеніе $abc...k$ дѣлитъ l.*

5. Всякое число k, дѣлящееся на оба числа a и b, называется общимъ кратнымъ чиселъ a и b. Изображая чрезъ d общій наибольшій дѣлитель чиселъ a и b, мы замѣчаемъ, что, во первыхъ, число $\frac{k}{d}$ дѣлится на оба числа $\frac{a}{d}$ и $\frac{b}{d}$, и, во вторыхъ, числа $\frac{a}{d}$ и $\frac{b}{d}$ суть относительно простыя; поэтому, на основаніи вышедоказаннаго, заключаемъ, что $\frac{k}{d}$ дѣлится на произведеніе $\frac{a}{d}\,\frac{b}{d}$. Пусть

Понятіе о наименьшемъ кратномъ.

$$\frac{k}{d}=\frac{a}{d}\,\frac{b}{d}\,t,$$

гдѣ t изображаетъ число цѣлое; отсюда выводимъ

$$k=\frac{ab}{d}t.$$

Эта формула даетъ всевозможныя общія кратныя чиселъ a и b; для этого стоитъ только поочередно полагать $t=1, 2, 3,...$

Наименьшее кратное получается при $t=1$; обозначая его чрезъ m, имѣемъ

$$m=\frac{ab}{d},$$

или

$$md=ab.$$

Характеристическое свойство наименьшаго общаго кратнаго чиселъ a и b состоитъ въ томъ, что *всякое общее кратное чиселъ a и b есть кратное ихъ наименьшаго кратнаго.* Ибо предыдущую формулу для k можно написать такъ:

$$k=mt.$$

Отмѣтимъ еще частный случай, когда числа a и b относительно простыя; тогда наименьшее кратное равно ихъ произведенію,

$$m = ab.$$

Если составимъ наименьшее кратное m' чиселъ a и b, а затѣмъ наименьшее кратное m чиселъ m' и c, то m будетъ очевидно наименьшимъ общимъ кратнымъ чиселъ a, b и c. Всякое другое общее кратное этихъ же самыхъ чиселъ будетъ дѣлиться на m. Если числа a, b, c простыя между собою, то $m = abc$.

Подобнымъ образомъ составляется наименьшее общее кратное четырехъ чиселъ, пяти и такъ далѣе.

§ II. Разложеніе чиселъ на простые множители.

Понятие о простых числах; число простых чисел безконечно.

6. Число, не имѣющее другихъ дѣлителей кромѣ единицы и самаго себя, называется *простымъ*. Самое малое простое число есть 2; оно одно между простыми числами есть четное. Единица не причисляется къ простымъ числамъ. Непростое число называется *составнымъ*; но единица отнюдь не причисляется къ составнымъ числамъ: она остается въ сторонѣ. Оставляя единицу въ сторонѣ, очевидно, что наименьшій изъ дѣлителей какого угодно даннаго числа есть всегда число простое; поэтому если число a не дѣлится ни на одно изъ *простыхъ* чиселъ меньшихъ a, то оно есть простое. Основываясь на этомъ предложеніи, легко показать, что существуетъ безконечное множество простыхъ чиселъ. На самомъ дѣлѣ, допустимъ противное, пусть $p_1, p_2, \ldots p_r$ изображаютъ всѣ существующія простыя числа; тогда число

теорема Евклида.

$$N = p_1 p_2 \ldots p_r + 1$$

очевидно не будетъ дѣлиться ни на одно изъ простыхъ чиселъ меньшихъ N, и потому само должно быть числомъ простымъ. Но это противорѣчитъ допущенію, что нѣтъ болѣе простыхъ чиселъ, кромѣ p_1, $p_2, \ldots p_r$.

7. Общимъ наибольшимъ дѣлителемъ простаго числа p и какого нибудь другаго числа a очевидно можетъ быть только 1 или p; если поэтому p не дѣлитъ a, то p и a суть относительно простыя.

Основныя свойства простыхъ чиселъ.

Это приводитъ къ слѣдующей теоремѣ.

Теорема. *Произведеніе* какихъ либо *нѣсколькихъ чиселъ $ab\ldots c$ тогда только дѣлится на простое число p, когда по крайней мѣрѣ одинъ изъ множителей $a, b, \ldots c$ дѣлится на p.*

Дѣйствительно, если ни одинъ изъ множителей $a, b, \ldots c$ не дѣлится на p, то каждый изъ нихъ есть число простое относительно p; слѣдовательно и произведеніе $ab\ldots c$ есть простое относительно p (см. n^0 4, слѣдствіе изъ теоремы 1), и потому не можетъ дѣлиться на p. Напротивъ, если одинъ изъ множителей $a, b, \ldots c$ дѣлится на p, то произведеніе $ab\ldots c$ очевидно дѣлится на p.

доказательство от противнаго.

Слѣдствіе. *Произведеніе нѣсколькихъ простыхъ множителей $pq\ldots r$ тогда только дѣлится на простое число s, когда одинъ изъ множителей $p, q, \ldots r$ равенъ s.*

Очевидно, что всякое число можетъ быть представлено въ видѣ произведенія нѣсколькихъ простыхъ множителей; относительно такого разложенія не трудно намъ теперь доказать слѣдующую теорему.

Теорема 2. *Не обращая вниманія на порядокъ множителей, всякое число разлагается однимъ только образомъ на произведеніе простыхъ множителей.*

Дѣйствительно, допустивъ, что число a разлагается двоякимъ образомъ на произведеніе простыхъ множителей

$$a = p_1 p_2 \ldots p_m,$$

$$a = q_1 q_2 \ldots q_n;$$

имѣемъ уравненіе

$$p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n,$$

первая ~~вторая~~ часть котораго дѣлится на p_1. Это требуетъ, чтобы одинъ изъ простыхъ множителей $q_1, q_2, \ldots q_n$ былъ равенъ p_1. Пусть $p_1 = q_1$; сокращаемъ обѣ части послѣдняго уравненія на p_1; получаемъ новое уравненіе

$$p_2 \ldots p_m = q_2 \ldots q_n,$$

на основаніи котораго заключаемъ, что одно изъ чиселъ q_2, $q_3, \ldots q_n$ равно p_2. Пусть $p_2 = q_2$; сокращаемъ обѣ части послѣдняго уравненія на p_2, и продолжаемъ разсуждать подобно предыдущему. Ясно, что такимъ образомъ мы дойдемъ до уравненія $1 = 1$, а это и показываетъ, что два ряда чиселъ

$$p_1, p_2, \ldots p_m$$

и

$$q_1, q_2, \ldots q_n$$

состоятъ изъ однихъ и тѣхъ же чиселъ; вся разница можетъ быть только въ порядкѣ. Что и слѣдовало доказать.

Когда число большое, разложеніе его на простые множители представляетъ значительныя затрудненія. Для чиселъ, не превышающихъ 3036000 можно пользоваться таблицами Бюркарда подъ заглавіемъ: «Table des diviseurs pour tous les nombres des premier, deuxième et troisième million etc. par J.-Ch. Burckhardt».

§ III. Условія дѣлимости и другія теоремы, вытекающія изъ предыдущаго.

8. Оставляя въ сторонѣ трудности, встрѣчаемыя при разложеніи большихъ чиселъ на простые множители, мы будемъ разсматривать какъ извѣстные всѣ простые дѣлители даннаго числа. Обозначая число чрезъ a, а различные простые дѣлители его чрезъ $p, q, \ldots r$, имѣемъ

$$(1) \ldots\ldots\ldots\ldots \quad a = p^\alpha q^\beta \ldots r^\gamma,$$

гдѣ α, β, . . . γ изображаютъ цѣлыя положительныя числа; это *показатели кратности* соотвѣтствующихъ простыхъ множителей.

Вопросъ о составленіи всѣхъ дѣлителей числа a не представляетъ теперь никакого затрудненія. На самомъ дѣлѣ, если b дѣлитъ a, то имѣемъ уравненіе

$$a = bb',$$

которое показываетъ, что дѣлитель b равенъ произведенію нѣсколькихъ простыхъ множителей, входящихъ въ составъ числа a; ибо всякое число, по вышедоказанному, однимъ только образомъ разлагается на произведеніе простыхъ множителей. Слѣдовательно будемъ имѣть

$$(2) \ldots\ldots\ldots\ldots \quad b = p^{\alpha'} q^{\beta'} \ldots r^{\gamma'},$$

гдѣ p, q, . . . r изображаютъ тѣ же простыя числа что и въ (1), а показатели α', β', . . . γ' удовлетворяютъ условіямъ

$$(3) \ldots\ldots\ldots\ldots \quad \begin{cases} 0 \leqq \alpha' \leqq \alpha, \\ 0 \leqq \beta' \leqq \beta, \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ 0 \leqq \gamma' \leqq \gamma. \end{cases}$$

Обратно, всякое число вида (2), при соблюденіи условій (3), будетъ дѣлителемъ числа a. Отсюда такая теорема.

Теорема. *Число a тогда только будетъ дѣлиться на b, когда всѣ простые множители числа b будутъ входить въ составъ a и въ a степени ихъ не ниже чѣмъ въ b.*

Слѣдствіе. *Число различныхъ дѣлителей числа $a = p^\alpha q^\beta \ldots r^\gamma$ есть $(\alpha + 1)(\beta + 1) \ldots (\gamma + 1)$, а сумма ихъ есть*

$$\frac{p^{\alpha+1} - 1}{p - 1} \cdot \frac{q^{\beta+1} - 1}{q - 1} \cdots \frac{r^{\gamma+1} - 1}{r - 1}.$$

На самомъ дѣлѣ, всѣ дѣлители числа a получаются изъ формулы

$$b = p^{\alpha'} q^{\beta'} \ldots r^{\gamma'},$$

давая для $\alpha', \beta', \ldots \gamma'$ значенія:

$$\alpha' = 0,\ 1,\ 2, \ldots \alpha,$$

$$\beta' = 0,\ 1,\ 2, \ldots \beta,$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\gamma' = 0,\ 1,\ 2, \ldots \gamma;$$

отсюда слѣдуетъ, что если перемножимъ алгебраически между собою полиномы

$$P = 1 + p + p^2 + \ldots + p^\alpha,$$

$$Q = 1 + q + q^2 + \ldots + q^\beta,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$R = 1 + r + r^2 + \ldots + r^\gamma,$$

то члены полученнаго произведенія будутъ представлять различные дѣлители числа a, каждый по одному разу; поэтому число дѣлителей числа a равно числу членовъ означеннаго произведенія, то есть

$$(\alpha + 1)(\beta + 1) \ldots (\gamma + 1),$$

а сумма ихъ опредѣляется произведеніемъ

$$P\,Q \ldots R,$$

которое равно

$$\frac{p^{\alpha+1} - 1}{p - 1} \, \frac{q^{\beta+1} - 1}{q - 1} \ldots \frac{r^{\gamma+1} - 1}{r - 1};$$

ибо

$$P = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$

$$Q = 1 + q + q^2 + \ldots + q^\beta = \frac{q^{\beta+1} - 1}{q - 1},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$R = 1 + r + r^2 + \ldots + r^\gamma = \frac{r^{\gamma+1} - 1}{r - 1}.$$

9. Въ нѣкоторыхъ случаяхъ приходится принимать во вниманіе наибольшее цѣлое число, не превышающее какого нибудь даннаго положительнаго количества ω; такое число называютъ цѣлою частью ω, и изображаютъ символомъ $E\omega$. Такъ, напримѣръ, имѣемъ

Наибольшая степень p, дѣлящая произведеніе 1.2.3...n.
Entier — цѣлое.

$$E\frac{1}{2} = 0, \quad E3 = 3, \quad E\frac{20}{7} = 2, \quad E\sqrt{150} = 12.$$

Рядомъ съ этимъ знакомъ мы введемъ еще другой, именно $e(\omega)$, понимая подъ послѣднимъ одно изъ двухъ: нуль или единицу, смотря по тому, будетъ ли $\omega < 1$ или $\omega \geq 1$. Напримѣръ,

$$e\left(\frac{2}{3}\right) = 0, \quad e(1) = 1, \quad e\left(\frac{3}{2}\right) = 1, \quad e(\sqrt{15}) = 1.$$

Для всякаго положительнаго количества x имѣетъ мѣсто равенство

$$Ex = e(x) + e\left(\frac{x}{2}\right) + e\left(\frac{x}{3}\right) + \ldots + e\left(\frac{x}{n}\right) + \ldots,$$

справедливость котораго очевидна.x) Члены ряда во второй части, начиная съ извѣстнаго мѣста, всѣ равны нулю; поэтому рядъ можетъ быть продолженъ до безконечности.

При нижеслѣдующихъ выводахъ намъ придется пользоваться обоими символическими выраженіями $E(x)$ и $e(x)$.

А. Теорема. *Наивысшая степень простаго числа p, дѣлящая произведеніе 1. 2. 3. 4 . . . n есть*

$$p^{E\frac{n}{p} + E\frac{n}{p^2} + E\frac{n}{p^3} + \ldots};$$

x) Положивъ $n \leqq x < n+1$, находимъ, что [illegible] членъ, не равный нулю, есть $e\left(\frac{x}{n}\right)$, [illegible], начиная съ $e\left(\frac{x}{n+1}\right)$ [illegible] равны нулю.

при этомъ рядъ членовъ въ показатель слѣдуетъ продолжать до тѣхъ поръ, пока онъ не окончится самъ собою.

Въ случаѣ $p > n$, число p не дѣлитъ произведенія $1.\,2.\,3\ldots n$, и теорема очевидна; поэтому слѣдуетъ предполагать при доказательствѣ, что $p \leqq n$.

Въ ряду $1,\,2,\,3,\ldots n$ числа, дѣлящіяся на p, суть слѣдующія:

$$p,\ 2p,\ 3p,\ldots n_1 p,$$

гдѣ n_1 изображаетъ наибольшее цѣлое число, не превышающее отношенія $\frac{n}{p}$, то есть

$$n_1 = E\frac{n}{p}.$$

Вслѣдствіе этого замѣчанія можно написать

$$(1) \ldots\ldots 1.\,2.\,3\ldots n = p^{n_1}\,1.\,2.\,3\ldots n_1\,a_1,$$

гдѣ a_1 изображаетъ цѣлое число, не дѣлящееся на p.

Допустимъ, что $p \leqq n_1$ и примѣнимъ формулу (1) къ произведенію $1.\,2.\,3\ldots n_1$; получаемъ

$$(2) \ldots\ldots 1.\,2.\,3\ldots n_1 = p^{n_2}\,1.\,2.\,3\ldots n_2\,a_2,$$

гдѣ a_2 изображаетъ число, не дѣлящееся на p, а n_2 опредѣляется по формулѣ

$$n_2 = E\frac{n_1}{p}.$$

Если $p \leqq n_2$, примѣняемъ формулу (1) къ произведенію $1.\,2.\,3\ldots n_2$; получаемъ

$$(3) \ldots\ldots 1.\,2.\,3\ldots n_2 = p^{n_3}\,1.\,2.\,3\ldots n_3\,a_3,$$

гдѣ a_3 изображаетъ число, не дѣлящееся на p, а n_3 опредѣляется по формулѣ

$$n_3 = E\frac{n_2}{p}.$$

Продолжая дѣйствовать такимъ образомъ, мы замѣчаемъ, что числа

$$n,\ n_1,\ n_2, \ldots$$

идутъ убывая; съ нѣкотораго мѣста они обращаются въ нуль. Пусть первое изъ нихъ, равное нулю, будетъ n_m; тогда очевидно

$$n_m = E\frac{n_{m-1}}{p}$$

$$n_{m-1} < p,$$

и уравненіе

$$(4) \ldots 1.\ 2.\ 3 \ldots n_{m-2} = p^{n_{m-1}}\, 1.\ 2.\ 3 \ldots n_{m-1} a_{m-1}$$

будетъ послѣднимъ въ ряду уравненій (1), (2), (3), . . . (4).

Перемножая почленно предыдущія уравненія и отбрасывая въ обѣихъ частяхъ общіе множители, получаемъ

$$1.2.3 \ldots n = p^{n_1 + n_2 + \ldots + n_{m-1}} a_1 a_2 \ldots a_{m-1}\, 1.2.3 \ldots n_{m-1},$$

или, проще,

$$1.\ 2.\ 3 \ldots n = p^{n_1 + n_2 + \ldots + n_{m-1}} a,$$

гдѣ a изображаетъ число, не дѣлящееся на p.

Отсюда видно, что простой множитель p входитъ въ составъ числа $1.\ 2.\ 3 \ldots n$ съ показателемъ

$$n_1 + n_2 + \ldots + n_{m-1}.$$

Послѣднее выраженіе можно продолжить какъ угодно далеко, даже можно представить въ видѣ безконечнаго ряда

$$n_1 + n_2 + \ldots + n_{m-1} + n_m + \ldots,$$

ибо всѣ члены, начиная съ n_m, равны нулю.

Числа n, n_1, n_2, . . . получаются однѣ изъ другихъ по слѣдующей общей формулѣ

$$n_{i+1} = E\frac{n_i}{p}, \quad (i = 0,\ 1,\ 2, \ldots);$$

если поэтому обозначимъ чрезъ $r, r_1, r_2, \ldots$ остатки, получаемые отъ дѣленія чиселъ $n, n_1, n_2, \ldots$ на p, то будемъ имѣть такой рядъ уравненій:

$$\frac{n}{p} = n_1 + \frac{r}{p}, \qquad \frac{n}{p^i} = \frac{n_1}{p^{i-1}} + \frac{r}{p^i}$$

$$\frac{n_1}{p} = n_2 + \frac{r_1}{p}, \qquad \frac{n_1}{p^{i-1}} = \frac{n_2}{p^{i-2}} + \frac{r_1}{p^{i-1}}$$

$$\frac{n_2}{p} = n_3 + \frac{r_2}{p}, \qquad \frac{n_2}{p^{i-2}} = \frac{n_3}{p^{i-3}} + \frac{r_2}{p^{i-2}}$$

$$\ldots\ldots\ldots, \qquad \ldots\ldots\ldots$$

$$\ldots\ldots\ldots, \qquad \ldots\ldots\ldots$$

откуда выводимъ по сложеніи

$$\frac{n}{p^i} = n_i + \frac{r + r_1 p + \ldots + r_{i-1} p^{i-1}}{p^i}.$$

$\leq p-1$

Но такъ какъ каждый изъ остатковъ $r, r_1, r_2, \ldots$ меньше p, то

$$r + r_1 p + \ldots + r_{i-1} p^{i-1} \leq (1 + p + \ldots + p^{i-1})(p-1), = \frac{p^i - 1}{p-1}(p-1) = p^i - 1$$

или

ибо всегда $r > 0$

$$0 < r + r_1 p + \ldots + r_{i-1} p^{i-1} \leq p^i - 1,$$

$$0 < \frac{n}{p^i} - n_i \leq \frac{p^i - 1}{p^i} = 1 - \frac{1}{p^i} < 1$$

и слѣдовательно

$$0 \leq \frac{n}{p^i} - n_i < 1.$$

Это показываетъ, что

$$n_i = E\frac{n}{p^i},$$

вслѣдствіе чего сумму

$$n_1 + n_2 + n_3 + \ldots$$

можно написать такъ:

$$E\frac{n}{p} + E\frac{n}{p^2} + E\frac{n}{p^3} + \ldots,$$

и теорема такимъ образомъ доказана.

Слѣдствіе. *Если $n = a + b + \ldots + c$, то отношеніе*

$$\frac{1.2.3\ldots n}{(1.2\ldots a)(1.2\ldots b)\ldots(1.2\ldots c)}$$

есть число цѣлое.

Дѣйствительно, пусть p означаетъ какое либо изъ простыхъ множителей, входящихъ въ составъ знаменателя. Изъ уравненія

$$n = a + b + \ldots + c,$$

какъ слѣдствіе, вытекаетъ рядъ такихъ неравенствъ:

$$E\frac{n}{p} \geqq E\frac{a}{p} + E\frac{b}{p} + \ldots + E\frac{c}{p},$$

$$E\frac{n}{p^2} \geqq E\frac{a}{p^2} + E\frac{b}{p^2} + \ldots + E\frac{c}{p^2},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Отсюда, складывая неравенства почленно, получаемъ

$$E\frac{n}{p} + E\frac{n}{p^2} + \ldots \geqq E\frac{a}{p} + E\frac{a}{p^2} + \ldots$$

$$+ E\frac{b}{p} + E\frac{b}{p^2} + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$+ E\frac{c}{p} + E\frac{c}{p^2} + \ldots$$

Послѣднее неравенство показываетъ, что p входитъ въ составъ числителя съ показателемъ не ниже, чѣмъ въ составъ знаменателя. Слѣдовательно въ настоящемъ случаѣ условія дѣлимости числителя на знаменатель удовлетворены.

В.10. **Теорема.** *Пусть $P(x)$ изображаетъ произведеніе всѣхъ цѣлыхъ чиселъ, не превышающихъ количества x,*[x] *а $\pi(x)$ — произведеніе всѣхъ простыхъ чиселъ, не превышающихъ x; въ случаѣ $x < 2$ слѣдуетъ подразумѣвать $P(x) = \pi(x) = 1$.*

x) при чемъ x можетъ быть не цѣлое.

При такомъ обозначеніи имѣетъ мѣсто слѣдующее равенство:

$$P(x) = \pi(x)\pi\left(\frac{x}{2}\right)\pi\left(\frac{x}{3}\right)\ldots$$
$$\pi(\sqrt{x})\,\pi\left(\sqrt{\frac{x}{2}}\right)\pi\left(\sqrt{\frac{x}{3}}\right)\ldots$$
$$\pi(\sqrt[3]{x})\,\pi\left(\sqrt[3]{\frac{x}{2}}\right)\pi\left(\sqrt[3]{\frac{x}{3}}\right)\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Въ каждой строкѣ во второй части слѣдуетъ остановиться на множителѣ равномъ 1; *число строкъ опредѣляется наименьшимъ цѣлымъ числомъ r, удовлетворяющимъ неравенству $x < 2^r$.*

Для доказательства обозначимъ чрезъ $p_1, p_2, p_3, \ldots$ простыя числа въ натуральномъ ихъ порядкѣ, такъ что $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ и т. д., и напишемъ разложеніе произведенія $1.\,2.\,3\ldots n$ на простые множители

$$1.\,2.\,3\ldots n = \left(p_1^{E\frac{n}{p_1} + E\frac{n}{p_1^2} + \ldots}\right)\left(p_2^{E\frac{n}{p_2} + E\frac{n}{p_2^2} + \ldots}\right)\ldots,$$

или, проще, такъ:

$$1.\,2.\,3\ldots n = \prod_i p_i^{E\frac{n}{p_i} + E\frac{n}{p_i^2} + \ldots},$$

гдѣ знакъ произведенія простирается на значенія $i = 1, 2, 3, \ldots$.

Подставивъ здѣсь на мѣсто знака E его выраженіе по формулѣ (см. n^0 9)

$$E(x) = e(x) + e\left(\frac{x}{2}\right) + e\left(\frac{x}{3}\right) + \ldots,$$

получаемъ

$$1.\,2.\,3\ldots n = \prod_i p_i^{e\left(\frac{n}{p_i}\right) + e\left(\frac{n}{2p_i}\right) + e\left(\frac{n}{3p_i}\right) + \ldots}$$
$$\prod_i p_i^{e\left(\frac{n}{p_i^2}\right) + e\left(\frac{n}{2p_i^2}\right) + \ldots}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Это удобнѣе представить такъ:

$$1.\ 2.\ 3\ldots n = \prod_i p_i^{e\left(\frac{n}{p_i}\right)} \prod_i p_i^{e\left(\frac{n}{2p_i}\right)} \prod_i p_i^{e\left(\frac{n}{3p_i}\right)} \ldots$$

$$\prod_i p_i^{e\left(\frac{n}{p_i^2}\right)} \prod_i p_i^{e\left(\frac{n}{2p_i^2}\right)} \prod_i p_i^{e\left(\frac{n}{3p_i^2}\right)} \ldots$$

$$\prod_i p_i^{e\left(\frac{n}{p_i^3}\right)} \prod_i p_i^{e\left(\frac{n}{2p_i^3}\right)} \prod_i p_i^{e\left(\frac{n}{3p_i^3}\right)} \ldots$$

. . . .

. . . .

Общее выраженіе множителей во второй части есть

$$\prod_i p_i^{e\left(\frac{n}{sp_i^r}\right)} = p_1^{e\left(\frac{n}{sp_1^r}\right)} p_2^{e\left(\frac{n}{sp_2^r}\right)} p_3^{e\left(\frac{n}{sp_3^r}\right)} \ldots,$$

и ясно, что оно представляетъ произведеніе всѣхъ простыхъ чиселъ, удовлетворяющихъ неравенству

$$\frac{n}{sp_i^r} \geqq 1,$$

или, одно и то же,

$$p_i \leqq \sqrt[r]{\frac{n}{s}}.$$

Поэтому можно написать

$$\prod_i p_i^{e\left(\frac{n}{sp_i^r}\right)} = \pi\left(\sqrt[r]{\frac{n}{s}}\right).$$

Внося во вторую часть предыдущаго равенства на мѣсто каждаго множителя соотвѣтствующее ему выраженіе по послѣдней формулѣ, получаемъ

$$1.\,2.\,3\ldots n = \pi(n)\,\pi\left(\frac{n}{2}\right)\pi\left(\frac{n}{3}\right)\ldots$$
$$\pi(\sqrt{n})\,\pi\left(\sqrt{\frac{n}{2}}\right)\pi\left(\sqrt{\frac{n}{3}}\right)\ldots$$
$$\pi(\sqrt[3]{n})\,\pi\left(\sqrt[3]{\frac{n}{2}}\right)\pi\left(\sqrt[3]{\frac{n}{3}}\right)\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Это и есть та формула, которую намъ слѣдовало вывести; только здѣсь мы имѣемъ частный случай: $x = n$ есть число цѣлое. Остается слѣдовательно провѣрить справедливость теоремы въ томъ предположенiи, что количество x содержится между двумя цѣлыми числами n и $n+1$,

$$n < x < n+1.$$

Для этого замѣчаемъ, что нѣтъ такого цѣлаго числа k, которое удовлетворяло бы неравенствамъ

$$\sqrt[r]{\frac{n}{s}} < k \leqq \sqrt[r]{\frac{x}{s}},$$

ибо въ противномъ случаѣ мы имѣли бы

$$n < sk^r \leqq x, < n+1$$

т.е. цѣлаго числа, заключеннаго между n и x.
что невозможно по предположенiю. Слѣдовательно

$$\pi\left(\sqrt[r]{\frac{x}{s}}\right) = \pi\left(\sqrt[r]{\frac{n}{s}}\right).$$

Внося во вторую часть предыдущаго равенства на мѣсто каждаго множителя его выраженiе по послѣдней формулѣ, и замѣчая, что первая часть равна $P(x)$, получаемъ

$$(1) \ldots\ldots P(x) = \pi(x)\,\pi\left(\frac{x}{2}\right)\pi\left(\frac{x}{3}\right)\ldots$$
$$\pi(\sqrt{x})\,\pi\left(\sqrt{\frac{x}{2}}\right)\pi\left(\sqrt{\frac{x}{3}}\right)\ldots$$
$$\pi(\sqrt[3]{x})\,\pi\left(\sqrt[3]{\frac{x}{2}}\right)\pi\left(\sqrt[3]{\frac{x}{3}}\right)\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Что и слѣдовало доказать.

Слѣдствіе 1. *Изображая чрезъ $T(x)$ сумму логариѳмовъ всѣхъ цѣлыхъ чиселъ, не превышающихъ количества x, а чрезъ $\theta(x)$ сумму логариѳмовъ всѣхъ простыхъ чиселъ, не превышающихъ x, имѣемъ*

$$(2) \ldots T(x) = \theta(x) + \theta\left(\frac{x}{2}\right) + \theta\left(\frac{x}{3}\right) + \ldots$$
$$+\,\theta(\sqrt{x}) + \theta\left(\sqrt{\frac{x}{2}}\right) + \theta\left(\sqrt{\frac{x}{3}}\right) + \ldots$$
$$+\,\theta(\sqrt[3]{x}) + \theta\left(\sqrt[3]{\frac{x}{2}}\right) + \theta\left(\sqrt[3]{\frac{x}{3}}\right) + \ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Въ случаѣ $x < 2$ слѣдуетъ полагать $T(x) = \theta(x) = 0$.

Равенство это получается непосредственно изъ (1) логариѳмированіемъ обѣихъ частей. Мы отмѣчаемъ его здѣсь потому, что въ извѣстныхъ изысканіяхъ форма (2) предпочитается (1).

Обозначая чрезъ $\psi(x)$ функцію

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \ldots,$$

имѣемъ

$$(3) \ldots\ldots T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \ldots$$

Важность равенства (2), или все равно (3), зависитъ отъ того, что оно даетъ средство для опредѣленія двухъ предѣловъ; между которыми заключается значеніе $\theta(x)$. Подобные предѣлы можно выводить съ помощью разныхъ пріемовъ, но не всѣ бу-

дутъ одинаково хороши; приходится предпочитать тѣ, которые ближе подходятъ къ дѣйствительному значенію $\theta(x)$. Здѣсь невозможно вдаваться въ подробности этого рода; читателя, желающаго ближе познакомиться съ сущностью предмета, отсылаемъ къ мемуару Чебышева о простыхъ числахъ, помѣщенному въ семнадцатомъ томѣ журнала Ліувиля. Однако, для примѣра, выведемъ одну формулу, вытекающую изъ (3) почти непосредственно; она заимствована изъ упомянутаго мемуара.

Слѣдствіе 2. *Имѣетъ мѣсто равенство*

$$
(4)\quad \left\{
\begin{aligned}
& T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right) \\
&= \psi(x)-\psi\left(\frac{x}{6}\right)+\psi\left(\frac{x}{7}\right)-\psi\left(\frac{x}{10}\right)+\psi\left(\frac{x}{11}\right)-\psi\left(\frac{x}{12}\right) \\
&+\psi\left(\frac{x}{13}\right)-\psi\left(\frac{x}{15}\right)+\psi\left(\frac{x}{17}\right)-\psi\left(\frac{x}{18}\right)+\psi\left(\frac{x}{19}\right)-\psi\left(\frac{x}{20}\right) \\
&+\psi\left(\frac{x}{23}\right)-\psi\left(\frac{x}{24}\right)+\psi\left(\frac{x}{29}\right)-\psi\left(\frac{x}{30}\right)+\psi\left(\frac{x}{31}\right)-\psi\left(\frac{x}{36}\right) \\
&+\psi\left(\frac{x}{37}\right)-\psi\left(\frac{x}{40}\right)+\ldots\ldots\ldots \\
&\ldots\ldots\ldots\ldots,
\end{aligned}
\right.
$$

гдѣ во второй части всѣ члены составляются изъ первыхъ шестнадцати, увеличивая послѣдовательно знаменатели 1, 6, 7, ... 30 *на* 30, *затѣмъ на* 60 и т. д.; *знаки чередуются попеременно.*

Изъ (3) выводимъ

$$
\begin{aligned}
& T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right) \\
&= \psi(x)+\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right)+\ldots \\
&+\psi\left(\frac{x}{30}\right)+\psi\left(\frac{x}{2.30}\right)+\psi\left(\frac{x}{3.30}\right)+\ldots \\
&-\psi\left(\frac{x}{2}\right)-\psi\left(\frac{x}{2.2}\right)-\psi\left(\frac{x}{2.3}\right)-\ldots \\
&-\psi\left(\frac{x}{3}\right)-\psi\left(\frac{x}{2.3}\right)-\psi\left(\frac{x}{3.3}\right)-\ldots \\
&-\psi\left(\frac{x}{5}\right)-\psi\left(\frac{x}{2.5}\right)-\psi\left(\frac{x}{3.5}\right)-\ldots
\end{aligned}
$$

Вторая часть этого равенства есть вида

$$A_1\psi(x) + A_2\psi\left(\frac{x}{2}\right) + A_3\psi\left(\frac{x}{3}\right) + \ldots,$$

гдѣ A_1, A_2, . . . изображаютъ цѣлые коэффиціенты.

Для опредѣленія A_n необходимо различать четыре случая:

1°. Если значекъ n не дѣлится ни на одно изъ чиселъ 2, 3, 5, тогда членъ $\psi\left(\frac{x}{n}\right)$ встрѣчается только одинъ разъ въ первой строкѣ, и потому имѣемъ $A_n = 1$.

2°. Если n дѣлится на одно только число изъ ряда 2, 3, 5, тогда членъ $\psi\left(\frac{x}{n}\right)$ встрѣчается два раза: въ первой строкѣ и въ одной изъ трехъ послѣднихъ строкъ; вслѣдствіе этого имѣемъ $A_n = 0$.

3°. Если n дѣлится на два числа въ ряду 2, 3, 5, а на третье не дѣлится, тогда $\psi\left(\frac{x}{n}\right)$ встрѣчается три раза: въ первой строкѣ и еще въ двухъ изъ трехъ послѣднихъ; поэтому имѣемъ $A_n = -1$.

4°. Если n дѣлится на 30, тогда $\psi\left(\frac{x}{n}\right)$ встрѣчается пять разъ: по одному разу въ каждой строкѣ; слѣдовательно $A_n = -1$.

Такимъ образомъ легко опредѣлить значеніе A_n; при этомъ слѣдуетъ замѣтить еще, что отъ увеличенія значка n на цѣлую кратность числа 30, значеніе коэффиціента A_n не мѣняется. На основаніи этого закона періодичности всѣ коэффиціенты A_n, начиная съ A_3, опредѣляются съ помощью нижеслѣдующей таблицы, содержащей значенія A_1, A_2, . . . до A_{30} включительно.

$A_1 = 1$,	$A_7 = 1$,	$A_{13} = 1$,	$A_{19} = 1$,	$A_{25} = 0$,
$A_2 = 0$,	$A_8 = 0$,	$A_{14} = 0$,	$A_{20} = -1$,	$A_{26} = 0$,
$A_3 = 0$,	$A_9 = 0$,	$A_{15} = -1$,	$A_{21} = 0$,	$A_{27} = 0$,
$A_4 = 0$,	$A_{10} = -1$,	$A_{16} = 0$,	$A_{22} = 0$,	$A_{28} = 0$,
$A_5 = 0$,	$A_{11} = 1$,	$A_{17} = 1$,	$A_{23} = 1$,	$A_{29} = 1$,
$A_6 = -1$,	$A_{12} = -1$,	$A_{18} = -1$,	$A_{24} = -1$,	$A_{30} = -1$.

Внося въ предыдущее равенство на мѣсто коеффиціентовъ A_1, A_2, . . . соотвѣтствующія числа, получаемъ ту формулу, которую слѣдовало доказать.

Характерное свойство формулы (4) состоитъ въ томъ, что во второй ея части знаки + и — взаимно чередуются. Принимая сверхъ того во вниманіе, что числовыя величины членовъ по свойству своему не могутъ возрастать, заключаемъ такія неравенства.

$$\psi(x)-\psi\left(\frac{x}{6}\right)\leqq T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)\leqq\psi(x).$$

Въ упомянутомъ выше мемуарѣ они играютъ весьма существенную роль.

Число чиселъ, простыхъ съ а и не превышающихъ а.

11. Во многихъ вопросахъ теоріи чиселъ необходимо принимать во вниманіе число чиселъ простыхъ относительно какого нибудь даннаго числа a и не превышающихъ a. Такое число принято изображать чрезъ $\varphi(a)$.

Если число a небольшое, значеніе $\varphi(a)$ можно опредѣлить непосредственно, такъ, напримѣръ, находимъ $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$, $\varphi(9)=6$, $\varphi(10)=4$ и т. д.

Значеніе функціи $\varphi(a)$ вычисляется легко съ помощью простыхъ множителей числа a. Для этого имѣемъ теорему:

Теорема. *Пусть будетъ какое угодно число*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_m^{\alpha_m}.$$

Число чиселъ простыхъ относительно a и не превышающихъ a опредѣляется по формулѣ

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_m}\right).$$

Теорема не имѣетъ мѣста въ случаѣ $a=1$, ибо 1 не разлагается на простые множители; но непосредственно видно, что $\varphi(1)=1$.

Если $a = p$ есть число простое, теорема очевидна; ибо тогда всѣ числа въ ряду 1, 2, 3,. . . a, за исключеніемъ послѣдняго, суть простыя относительно a; слѣдовательно въ этомъ случаѣ имѣемъ

считая также и 1 за число, простое съ a.

$$\varphi(a) = a - 1 = p\left(1 - \frac{1}{p}\right).$$

Равнымъ образомъ справедливость теоремы провѣряется очень легко и въ томъ случаѣ, когда число a есть степень простаго числа

$$a = p^{\alpha}.$$

Тогда числа, не превышающія a и не простыя съ a, суть слѣдующія:

$$p,\ 2p,\ 3p, \ldots, p^{\alpha-1}\cdot p = a.$$

Ихъ число есть $p^{\alpha-1}$, и если въ ряду

$$1,\ 2,\ 3, \ldots p^{\alpha}$$

вычеркнемъ всѣ тѣ числа, которыя содержатся въ предшествующемъ ряду, то оставшіяся представятъ всѣ числа простыя относительно a и не превышающія a. Число этихъ послѣднихъ есть $p^{\alpha} - p^{\alpha-1}$; слѣдовательно

$$\varphi(p^{\alpha}) = p^{\alpha}\left(1 - \frac{1}{p}\right) = a\left(1 - \frac{1}{p}\right).$$

Переходя теперь къ случаю, когда число простыхъ множителей, входящихъ въ составъ числа a, превышаетъ 1, т. е. $m > 1$, мы отмѣтимъ въ ряду

(1). . . . . 1, 2, 3, 4,. . . a

сперва всѣ тѣ числа, которыя не дѣлятся на p_1, ихъ число изобразимъ чрезъ $\psi(a; p_1)$; затѣмъ отмѣтимъ въ (1) всѣ тѣ числа, которыя не дѣлятся ни на p_1, ни на p_2, ихъ число изобразимъ чрезъ $\psi(n; p_1, p_2)$; послѣ этого отмѣтимъ всѣ числа, не дѣлящіяся ни на одно изъ чиселъ p_1, p_2, p_3, число ихъ изобразимъ чрезъ $\psi(n; p_1, p_2, p_3)$ и такъ далѣе.

Постараемся прежде всего опредѣлить число $\psi(a; p_1)$. Для этого выпишемъ отдѣльно всѣ числа, которыя содержатся въ (1) и дѣлятся на p_1:

$$(2) \ldots\ldots\ldots\ldots\ p_1,\ 2p_1,\ 3p_1, \ldots \frac{a}{p_1}p_1;$$

ихъ число есть $\frac{a}{p_1}$. Числа въ ряду (1), не заключающіяся во (2), не дѣлятся на p_1; ихъ число есть $a - \frac{a}{p_1}$; слѣдовательно

$$(3) \ldots\ldots\ldots\ldots\ \psi(a; p_1) = a\left(1 - \frac{1}{p_1}\right).$$

Всѣ тѣ числа въ (1), которыя не дѣлятся ни на одно изъ простыхъ чиселъ

$$p_1, p_2, p_3, \ldots p_i, \quad (i < m),$$

образуютъ двѣ группы: въ первую входятъ числа дѣлящіяся на p_{i+1}, во вторую остальныя, не дѣлящіяся на p_{i+1}.

Числа первой группы заключаются x) въ ряду

$$p_{i+1},\ 2p_{i+1},\ 3p_{i+1} \ldots \frac{a}{p_{i+1}}p_{i+1},$$

и отличаются тѣмъ, что не дѣлятся ни на одно изъ чиселъ p_1, $p_2, \ldots p_i$. Чтобы выдѣлить ихъ изъ послѣдняго ряда, слѣдуетъ отмѣтить въ ряду коеффиціентовъ

$$1,\ 2,\ 3, \ldots \frac{a}{p_{i+1}}$$

тѣ, которыя не дѣлятся ни на одно изъ чиселъ $p_1, p_2, \ldots p_i$. По вышепринятому обозначенію ихъ число выражается символомъ

$$\psi\left(\frac{a}{p_{i+1}}; p_1, p_2, \ldots p_i\right);$$

поэтому тѣмъ же символомъ выражается число чиселъ, образующихъ первую группу. Что касается чиселъ второй группы, то изъ самаго опредѣленія ихъ вытекаетъ, что число ихъ есть

$$\psi(a; p_1, p_2, \ldots p_{i+1}).$$

x) Заключаются, какъ часть этого ряда.

Число чиселъ, образующихъ обѣ группы, выражается символомъ

$$\psi(a;\, p_1,\, p_2,\, \ldots p_i);$$

слѣдовательно

$$\psi(a; p_1, p_2 \ldots p_i) = \psi\left(\frac{a}{p_{i+1}}; p_1, p_2 \ldots p_i\right) + \psi(a; p_1, p_2 \ldots p_{i+1})$$

или

$$(4)\quad \psi(a: p_1, p_2 \ldots p_{i+1}) = \psi(a; p_1, p_2 \ldots p_i) - \psi\left(\frac{a}{p_{i+1}}; p_1, p_2 \ldots p_i\right).$$

Полагая здѣсь $i = 1$, получаемъ

$$\psi(a;\, p_1,\, p_2) = \psi(a;\, p_1) - \psi\left(\frac{a}{p_2};\, p_1\right),$$

а это, по формулѣ (3), приводится къ слѣдующему

$$\psi(a;\, p_1,\, p_2) = a\left(1 - \frac{1}{p_1}\right) - \frac{a}{p_2}\left(1 - \frac{1}{p_1}\right),$$

или, проще,

$$(5) \ldots\ldots\ \psi(a,\, p_1,\, p_2) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).$$

Далѣе, полагая въ (4) $i = 2$, получаемъ

$$\psi(a;\, p_1,\, p_2,\, p_3) = \psi(a;\, p_1,\, p_2) - \psi\left(\frac{a}{p_3};\, p_1,\, p_2\right);$$

отсюда, внося во вторую часть на мѣсто обоихъ членовъ ихъ выраженія по формулѣ (5), находимъ

$$\psi(a;\, p_1,\, p_2,\, p_3) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) - \frac{a}{p_3}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right),$$

или, проще,

$$(6) \ldots\ \psi(a;\, p_1,\, p_2,\, p_3) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right).$$

Продолжая разсуждать подобнымъ образомъ, мы убѣждаемся въ справедливости общей формулы

$$(7)\quad \psi(a;\, p_1,\, p_2, \ldots p_i) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right).$$

Если теперь замѣтимъ, что числа простыя относительно a и не превышающія a заключаются въ ряду $1, 2, 3, \ldots a$ и не дѣлятся ни на одно изъ простыхъ чиселъ $p_1, p_2, \ldots p_m$, и что это составляетъ признакъ характеристическій означенныхъ чиселъ, то ясно, что $\varphi(a) = \psi(a; p_1, p_2, \ldots p_m)$. Слѣдовательно

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_m}\right).$$

Этимъ теорема доказана. Прибавимъ только, что послѣднюю формулу можно написать, не вводя дробей, такъ:

$$\varphi(a) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_m^{\alpha_m - 1} (p_1 - 1)(p_2 - 1) \ldots (p_m - 1).$$

Если выполнить умноженіе во второй части, то выраженіе $\varphi(a)$ представится въ видѣ полинома изъ 2^m членовъ; каждый членъ имѣетъ видъ цѣлаго одночлена

$$\pm p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}.$$

Половинѣ членовъ предшествуетъ коеффиціентъ $+1$, половинѣ -1. Изображая для сокращенія члены съ коеффиціентомъ $+1$ чрезъ $\lambda_1, \lambda_2, \ldots \lambda_{2^{m-1}}$, а члены съ коеффиціентомъ -1 чрезъ $\lambda'_1, \lambda'_2, \ldots \lambda'_{2^{m-1}}$, имѣемъ

$$\varphi(a) = \sum_i \lambda_i - \sum_i \lambda'_i, \quad (i = 1, 2, \ldots 2^{m-1}).$$

Для опредѣленія обоихъ суммъ, равно какъ и членовъ λ_1, λ'_1, λ_2, $\lambda'_2, \ldots$, служатъ формулы

$$\sum_i \lambda_i = a\left(1 + \sum \frac{1}{p_1 p_2} + \sum \frac{1}{p_1 p_2 p_3 p_4} + \ldots\right),$$

$$\sum_i \lambda'_i = a\left(\sum \frac{1}{p_1} + \sum \frac{1}{p_1 p_2 p_3} + \sum \frac{1}{p_1 p_2 p_3 p_4 p_5} + \ldots\right);$$

здѣсь знаки Σ во второй части изображаютъ суммы изъ произведеній элементовъ

$$\frac{1}{p_1}, \frac{1}{p_2}, \frac{1}{p_3}, \ldots \frac{1}{p_m},$$

сочетаемыхъ по одному, по два, по три и т. д. Напримѣръ, полагая

$$a=p_1^2p_2^3p_3,$$

находимъ

$$\sum\lambda_i=a\left(1+\sum\frac{1}{p_1p_2}\right)=p_1^2p_2^3p_3\left(1+\frac{1}{p_1p_2}+\frac{1}{p_1p_3}+\frac{1}{p_2p_3}\right),$$

$$\sum\lambda'_i=a\left(\sum\frac{1}{p_1}+\sum\frac{1}{p_1p_2p_3}\right)=p_1^2p_2^3p_3\left(\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}+\frac{1}{p_1p_2p_3}\right).$$

Слѣдовательно

$$\varphi(p_1^2p_2^3p_3)=p_1^2p_2^3p_3+p_1\,p_2^2p_3+p_1\,p_2^3+p_1^2p_2^2$$
$$-p_1\,p_2^3p_3-p_1^2p_2^2p_3-p_1^2p_2^3-p_1\,p_2^2.$$

12. **Теорема.** *Если числа a и b суть относительно простыя, то имѣетъ мѣсто равенство* Свойства функціи $\varphi(a)$ (первое).

$$\varphi(ab)=\varphi(a)\varphi(b).$$

Теорема эта есть слѣдствіе предыдущей, но можетъ быть доказана независимо; тогда, наоборотъ, предыдущая теорема будетъ слѣдствіемъ настоящей.

Считаемъ полезнымъ привести здѣсь оба доказательства.

Первое доказательство. Такъ какъ числа

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_m^{\alpha_m},\qquad b=q_1^{\beta_1}q_2^{\beta_2}\ldots q_n^{\beta_n}$$

относительно простыя, то ни одинъ изъ простыхъ множителей $p_1, p_2, \ldots$ не равенъ ни одному изъ множителей $q_1, q_2, \ldots$; поэтому въ произведеніи

$$ab=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_m^{\alpha_m}q_1^{\beta_1}q_2^{\beta_2}\ldots q_n^{\beta_n}$$

множители $p_1, p_2, \ldots q_n$ суть различные, и слѣдовательно

$$\varphi(ab)=ab\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_m}\right)\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_n}\right).$$

Переставляя множители во второй части, можно послѣднее равенство написать такъ:

$$\varphi(ab) = a\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_m}\right) b\left(1 - \frac{1}{q_1}\right)\ldots\left(1 - \frac{1}{q_n}\right),$$

а это очевидно приводится къ слѣдующему

$$\varphi(ab) = \varphi(a)\,\varphi(b),$$

и теорема такимъ образомъ доказана.

Второе доказательство. Напишемъ три ряда чиселъ,

$$0,\ 1,\ 2,\ 3, \ldots\ l, \ldots ab - 1;$$

$$0,\ 1,\ 2,\ 3, \ldots m, \ldots\ a - 1;$$

$$0,\ 1,\ 2,\ 3, \ldots\ n, \ldots\ b - 1;$$

и взявъ какое либо изъ чиселъ перваго ряда, положимъ l, раздѣлимъ его разъ на a, другой разъ на b; остатокъ отъ перваго дѣленія содержится во второмъ ряду, отъ втораго — въ третьемъ. Обозначивъ ихъ чрезъ m и n, имѣемъ

$$l = ah + m, \qquad l = bk + n.$$

Такимъ образомъ каждое изъ чиселъ въ первомъ ряду опредѣляетъ нѣкоторое, ему соотвѣтствующее сочетаніе (m, n) изъ одного числа втораго ряда съ однимъ числомъ третьяго ряда: Зависимость эта сопровождается слѣдующими обстоятельствами.

1°. *Различнымъ числамъ l соотвѣтствуютъ различныя пары (m, n).*

Дѣйствительно, допустимъ противное; пусть двумъ неравнымъ числамъ l и l' отвѣчаетъ одна и та же пара (m, n). Тогда будемъ имѣть уравненія

$$l = ah + m, \qquad l = bk + n,$$

$$l' = ah' + m, \qquad l' = bk' + n,$$

изъ которыхъ выводимъ

$$l - l' = a(h - h'), \qquad l - l' = b(k - k').$$

Отсюда заключаемъ, что разность $l - l'$ дѣлится на оба числа a и b. Но a и b относительно простыя; поэтому $l - l'$ дѣлится на ab, — заключенiе невозможное; ибо $l - l'$ не равно нулю и по числовой величинѣ меньше ab.

2°. *Для всякаго сочетанія* (m, n), *составленнаго изъ двухъ произвольно взятыхъ чиселъ, одно во второмъ ряду, другое въ третьемъ, найдется такое число* l *въ первомъ ряду, которое будетъ состоять съ* (m, n) *въ вышеуказанной зависимости.*

На самомъ дѣлѣ, опредѣливъ сочетанія (m, n), отвѣчающія всѣмъ числамъ въ первомъ ряду, мы будемъ имѣть ab *различныхъ* паръ (m, n), то есть ровно столько, сколько имѣется ихъ всѣхъ.

3°. *Если число* l *есть простое относительно* ab, *то въ соотвѣтствующей ему парѣ* (m, n) *число* m *есть простое относительно* a, *а* n *простое относительно* b.

Допустимъ противное; пусть a и m имѣютъ общій дѣлитель $d > 1$. Уравненіе

$$l = ah + m$$

l и a, а потому также

показываетъ, что тогда l дѣлится на d. Слѣдовательно l и ab имѣли бы общій дѣлитель d, что противорѣчитъ предположенію.

4°. *Если въ сочетаніи* (m, n) *число* m *есть простое относительно* a, *а число* n *простое относительно* b, *то соотвѣтствующее число* l *будетъ простымъ относительно* ab.

На самомъ дѣлѣ, изъ уравненій

$$l = ah + m, \qquad l = bk + n$$

первое показываетъ, что число l есть простое относительно a, второе — что l простое относительно b. Число l, будучи простымъ относительно каждаго изъ чиселъ a и b, есть простое относительно произведенія ab.

Принимая въ соображенiе все вышедоказанное, переходимъ теперь къ первому ряду, и выдѣлимъ изъ него всѣ числа простыя съ ab; пусть они будутъ

$$l, l', l'', \ldots l^{(i-1)}, \quad (i = \varphi(ab));$$

ихъ число равно $\varphi(ab)$. Составляемъ для каждаго изъ нихъ соотвѣтствующую пару

$$(m, n), (m', n'), (m'', n''), \ldots (m^{(i-1)}, n^{(i-1)}).$$

Эти пары будутъ представлять всевозможныя сочетанiя одного изъ чиселъ простыхъ относительно a и не превышающихъ a съ однимъ изъ чиселъ простыхъ относительно b и не превышающихъ b. Число такихъ сочетанiй очевидно есть $\varphi(a)\,\varphi(b)$; поэтому имѣемъ $i = \varphi(a)\,\varphi(b)$, то есть

$$\varphi(ab) = \varphi(a)\,\varphi(b).$$

Что и слѣдовало доказать.

Слѣдствiе. *Если $a, b, c, \ldots d$ суть числа относительно простыя, то*

$$\varphi(abc\ldots d) = \varphi(a)\,\varphi(b)\,\varphi(c)\ldots\varphi(d).$$

Это доказывается примѣненiемъ послѣдней теоремы нѣсколько разъ.

Полагая

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m},$$

на основанiи предыдущаго заключаемъ

$$\varphi(a) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2})\ldots\varphi(p_m^{\alpha_m}).$$

Отсюда видимъ, что съ помощью послѣдней теоремы вопросъ объ опредѣленiи $\varphi(a)$ при a сложномъ приводится къ частному случаю, когда a есть степень простаго числа; но тогда опредѣленiе $\varphi(a)$ не представляетъ никакого затрудненiя, какъ это было показано ранѣе.

Свойства функции φ(a) (второе).

13. Теорема. *Если всѣ дѣлители числа*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

обозначимъ чрезъ d, d_1, d_2, . . ., *то имѣетъ мѣсто такое равенство*:

$$\varphi(d) + \varphi(d_1) + \varphi(d_2) + \dots = a.$$

Эта теорема можетъ быть очень легко провѣрена, если воспользоваться извѣстными выраженіями количествъ $\varphi(d)$, $\varphi(d_1)$, . . .; не менѣе интересно и другое доказательство, непосредственное, не требующее, чтобы намъ было извѣстно выраженіе функціи $\varphi(a)$.

Мы изложимъ оба способа.

Первое доказательство. Перемножая между собой алгебраически m полиномовъ вида

$$1 + \varphi(p_i) + \varphi(p_i^2) + \dots + \varphi(p_i^{\alpha_i}),$$

гдѣ значекъ i принимаетъ послѣдовательно значенія $1, 2, 3, \dots m$, получаемъ въ результатѣ сумму

$$\sum \varphi(p_1^{\lambda_1})\, \varphi(p_2^{\lambda_2}) \dots \varphi(p_m^{\lambda_m}),$$

которая простирается на значенія показателей

$$0 \leqq \lambda_i < \alpha_i, \quad (i = 1, 2, 3, \dots m).$$

Такъ какъ простыя числа $p_1, p_2, \dots p_m$ всѣ различны, то послѣднее выраженіе можно написать такъ:

$$\sum \varphi(p_1^{\lambda_1} p_2^{\lambda_2} \dots p_m^{\lambda_m}),$$

а это въ свою очередь можно написать проще такъ:

$$\sum \varphi(d);$$

гдѣ знакъ суммы простирается на всѣ дѣлители числа a.

Итакъ, имѣемъ равенство

$$\prod_i \left(1 + \varphi(p_i) + \varphi(p_i^2) + \ldots + \varphi(p_i^{\alpha_i})\right) = \sum \varphi(d).$$

Съ другой стороны имѣемъ

$$1 + \varphi(p_i) + \varphi(p_i^2) + \ldots \varphi(p_i^{\alpha_i})$$
$$= 1 + (p_i - 1) + p_i(p_i - 1) + \ldots + p_i^{\alpha_i - 1}(p_i - 1)$$
$$= 1 + (p_i - 1)(1 + p_i + \ldots + p_i^{\alpha_i - 1})$$
$$= p_i^{\alpha_i};$$

слѣдовательно

$$\prod_i p_i^{\alpha_i} = \sum \varphi(d)$$

или, проще,

$$a = \sum \varphi(d).$$

Что и слѣдовало доказать.

Второе доказательство. Если d есть какой нибудь изъ дѣлителей числа a, то число чиселъ, не превышающихъ a и имѣющихъ съ a, каждое порознь, общій наибольшій дѣлитель d, есть $\varphi\left(\frac{a}{d}\right)$; ибо всѣ означенныя числа получаются изъ формулы

$$dt,$$

приравнивая въ ней перемѣнное t различнымъ числамъ, простымъ относительно $\frac{a}{d}$ и не превышающимъ $\frac{a}{d}$.

Возьмемъ теперь во вниманіе всѣ числа отъ 1 до a включительно, и распредѣлимъ ихъ на группы, согласившись предварительно зачислять къ одной и той же группѣ тѣ изъ нихъ, которыя съ числомъ a имѣютъ одинъ и тотъ же общій наибольшій дѣлитель. Число такихъ группъ равняется числу различныхъ дѣлителей числа a, и каждая изъ нихъ опредѣляется соотвѣтствующимъ дѣлителемъ d_j; число чиселъ, принадлежащихъ къ

одной и той же группѣ, есть $\varphi\left(\frac{a}{d_j}\right)$. Слѣдовательно число чиселъ во всѣхъ группахъ равняется суммѣ

$$\varphi\left(\frac{a}{d}\right)+\varphi\left(\frac{a}{d_1}\right)+\varphi\left(\frac{a}{d_2}\right)+\ldots,$$

и такимъ образомъ получаемъ равенство

$$\varphi\left(\frac{a}{d}\right)+\varphi\left(\frac{a}{d_1}\right)+\varphi\left(\frac{a}{d_2}\right)+\ldots=a,$$

которое можно написать просто такъ:

$$\varphi(d)+\varphi(d_1)+\varphi(d_2)+\ldots=a,$$

ибо числа $\frac{a}{d}, \frac{a}{d_1}, \frac{a}{d_2}, \ldots$ составляетъ нѣкоторое перемѣщеніе чиселъ $d, d_1, d_2, \ldots$ Послѣднее равенство есть именно то, которое слѣдовало доказать.

14. Полагая въ равенствѣ Рѣшеніе одной задачи.

$$(1) \ldots\ldots\ldots\ldots\ldots \sum_d \varphi(d)=a$$

$a=1, 2, 3, \ldots$ получаемъ рядъ такихъ уравненій:

$$\varphi(1)=1,$$
$$\varphi(1)+\varphi(2)=2,$$
$$\varphi(1)+\varphi(3)=3,$$
$$\varphi(1)+\varphi(2)+\varphi(4)=4,$$
$$\varphi(1)+\varphi(5)=5,$$
$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)=6,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Отсюда выводимъ

$$\varphi(1)=1, \quad \varphi(2)=1, \quad \varphi(3)=2, \quad \varphi(4)=2,$$
$$\varphi(5)=4, \quad \varphi(6)=2, \ldots$$

Слѣдовательно равенство (1) опредѣляетъ собою вполнѣ функцію $\varphi(a)$, и выраженіе послѣдней можетъ быть выведено какъ слѣдствіе изъ (1). Мы не будемъ однако останавливаться на этомъ, а прямо покажемъ рѣшеніе болѣе общей задачи, играющей существенную роль при нѣкоторыхъ изысканіяхъ въ алгебрѣ и теоріи чиселъ; вопросъ состоитъ въ томъ, чтобы по данной функціи $f(a)$ цѣлаго перемѣннаго a найти такую функцію $\psi(a)$, которая удовлетворяла бы равенству

$$(2) \ldots\ldots\ldots\ldots \sum_d \psi(d) = f(a),$$

гдѣ знакъ суммы относится ко всѣмъ дѣлителямъ d числа a.

Въ частномъ случаѣ, когда $f(a) = a$, имѣемъ $\psi(a) = \varphi(a)$. Прежде чѣмъ приступить къ общему рѣшенію, слѣдуетъ удостовѣриться, что равенство (2) вполнѣ опредѣляетъ собой искомую функцію $\psi(a)$. Для этого въ (2) полагаемъ послѣдовательно $a = 1, 2, 3, \ldots$; получаемъ

$$\begin{aligned}
&\psi(1) = f(1),\\
&\psi(1) + \psi(2) = f(2),\\
&\psi(1) + \psi(3) = f(3),\\
&\psi(1) + \psi(2) + \psi(4) = f(4),\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots,
\end{aligned}$$

откуда выводимъ

$$\begin{aligned}
&\psi(1) = f(1),\\
&\psi(2) = f(2) - f(1),\\
&\psi(3) = f(3) - f(1),\\
&\psi(4) = f(4) - f(2),\\
&\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots
\end{aligned}$$

Эти равенства даютъ возможность опредѣлить значеніе $\psi(a)$ при какомъ угодно a. Чтобы составить общее выраженіе функ-

ціи $\psi(a)$, подставляемъ въ обѣихъ частяхъ (1), на мѣсто a, d, $d_1, \ldots$ разложенія этихъ чиселъ на простые множители, обозначая эти послѣдніе буквами $p_1, p_2, \ldots$; затѣмъ на мѣсто $\varphi(d)$, $\varphi(d_1), \ldots$ подставимъ соотвѣтствующія выраженія по формуламъ

$$\varphi(d) = \Sigma\lambda - \Sigma\lambda',$$

$$\varphi(d_1) = \Sigma\mu - \Sigma\mu', \ldots$$

Вслѣдствіе этого равенство (1) принимаетъ видъ

$$(3) \ldots\ldots \sum_d [\Sigma\lambda - \Sigma\lambda'] = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m};$$

гдѣ обѣ части, относительно буквъ $p_1, p_2, \ldots p_m$, представляютъ цѣлыя функціи.

Но очевидно, что равенство (3) представляетъ тожество относительно буквъ $p_1, p_2, \ldots p_m$, разсматриваемыхъ какъ независимыя перемѣнныя; поэтому на мѣсто различныхъ одночленовъ въ обѣихъ частяхъ (3) можно подставлять какія угодно новыя количества, и равенство отъ этого не нарушится. Мы воспользуемся этимъ замѣчаніемъ слѣдующимъ образомъ. Обозначая чрезъ u любой членъ въ равенствѣ (3), взятый безъ предшествующаго ему знака, подставимъ $f(u)$ на мѣсто u, и примѣнимъ эту подстановку ко всѣмъ членамъ. По совершеніи такого дѣйствія получается новое равенство

$$\sum_d [\Sigma f(\lambda) - \Sigma f(\lambda')] = f(a).$$

Здѣсь разность двухъ суммъ

$$\Sigma f(\lambda) - \Sigma f(\lambda')$$

опредѣляется вполнѣ дѣлителемъ d; ее слѣдовательно можно разсматривать, какъ функцію цѣлаго перемѣннаго d, и если изобразить ее чрезъ $\psi(d)$, то послѣднее равенство принимаетъ видъ

$$\sum_d \psi(d) = f(a),$$

совпадающій съ (2). Это доказываетъ, что функція

$$\psi(d) = \Sigma f(\lambda) - \Sigma f(\lambda')$$

есть искомая, и такимъ образомъ получается слѣдующая теорема.

9. **Теорема.** *Пусть $f(a)$ изображаетъ произвольную функцію цѣлаго перемѣннаго a, $\psi(a)$ — искомую функцію, которая должна удовлетворять равенству*

$$\sum_d \psi(d) = f(a),$$

гдѣ знакъ суммы простирается на всѣ дѣлители числа a.

Для опредѣленія функціи $\psi(a)$ служитъ формула

$$\psi(a) = f(a) - \sum f\left(\frac{a}{p_1}\right) + \sum f\left(\frac{a}{p_1 p_2}\right) - \sum f\left(\frac{a}{p_1 p_2 p_3}\right) + \ldots,$$

гдѣ знаки суммы относятся къ различнымъ сочетаніямъ простыхъ дѣлителей $p_1, p_2, \ldots$ числа a, по одному, по два, по три и такъ далѣе.

Слѣдствіе. *Если $f(a)$ изображаетъ произвольную функцію цѣлаго перемѣннаго, а $\psi(a)$ — такую функцію, которая удовлетворяетъ равенству*

$$\prod_d \psi(d) = f(a),$$

гдѣ знакъ произведенія простирается на всѣ дѣлители числа a, то функція $\psi(a)$ опредѣляется посредствомъ $f(a)$ по слѣдующей формулѣ:

$$\psi(a) = \frac{f(a)\,\Pi f\left(\frac{a}{p_1 p_2}\right)\Pi f\left(\frac{a}{p_1 p_2 p_3 p_4}\right)\ldots}{\Pi f\left(\frac{a}{p_1}\right)\Pi f\left(\frac{a}{p_1 p_2 p_3}\right)\ldots},$$

гдѣ знаки произведенія простираются на различныя сочетанія изъ простыхъ множителей числа a по одному, по два и т. д.

Дѣйствительно, принявъ $\log f(a)$ за данную функцію, и обозначивъ чрезъ $\log \psi(a)$ искомую функцію, которая должна удовлетворять равенству

$$\sum_d \log \psi(d) = \log f(a),$$

для опредѣленія $\log \psi(a)$ имѣемъ формулу

$$\log \psi(a) = \log f(a) - \sum \log f\left(\frac{a}{p_1}\right) + \sum \log f\left(\frac{a}{p_1 p_2}\right) - \ldots$$

Если перейдемъ отъ логариѳмовъ къ числамъ, то справедливость слѣдствія обнаружится непосредственно.

15. *Примѣръ 1. Положимъ, что для всякаго значенія перемѣннаго x имѣетъ мѣсто равенство* Примѣры.

$$T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \ldots;$$

тогда функція $\psi(x)$ можетъ быть выражена чрезъ $T(x)$ по формулѣ

$$\psi(x) = A_1 T(x) + A_2 T\left(\frac{x}{2}\right) + A_3 T\left(\frac{x}{3}\right) + \ldots,$$

гдѣ A_1, A_2, ... суть неизвѣстные коеффиціенты, которые требуется опредѣлить.

Вносся во вторую часть послѣдняго равенства, на мѣсто $T(x)$, $T\left(\frac{x}{2}\right)$, ... соотвѣтствующія выраженія, получаемыя изъ предшествующей формулы, и затѣмъ, приравнивая между собою коеффиціенты въ обѣихъ частяхъ у $\psi(x)$, у $\psi\left(\frac{x}{2}\right)$, у $\psi\left(\frac{x}{3}\right)$ и т. д., получаемъ рядъ уравненій:

$$A_1 = 1,$$
$$A_1 + A_2 = 0,$$
$$A_1 + A_3 = 0,$$
$$A_1 + A_2 + A_4 = 0,$$
$$\ldots\ldots\ldots\ldots,$$

которыя, за исключеніемъ перваго, получаются изъ общей формы

$$\sum_d A_d = 0,$$

гдѣ знакъ суммы простирается на всѣ дѣлители числа n. Изображая слѣдовательно чрезъ $f(n)$ функцію цѣлаго перемѣннаго n, которая при $n=1$ равна 1, а при $n>1$ равна нулю, можемъ написать

$$\sum_d A_d = f(n),$$

гдѣ знакъ суммы простирается на всѣ дѣлители числа n.

На основаніи вышедоказанной теоремы изъ послѣдняго равенства выводимъ

$$A_n = f(n) - \sum f\left(\frac{n}{p_1}\right) + \sum f\left(\frac{n}{p_1 p_2}\right) - \ldots$$

Отсюда заключаемъ слѣдующее.

1°. Если въ составъ числа n входитъ по крайней мѣрѣ одинъ простой множитель съ показателемъ выше 1, то

$$A_n = 0.$$

2°. Если въ составъ числа n входитъ μ различныхъ простыхъ множителей, каждый съ показателемъ равнымъ 1, то

$$A_n = (-1)^\mu.$$

Внося въ выраженіе функціи $\psi(x)$ на мѣсто коеффиціентовъ $A_1, A_2, \ldots$ ихъ значенія, получаемъ формулу

$$\psi(x) = T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) + T\left(\frac{x}{6}\right) - T\left(\frac{x}{7}\right)$$
$$+ T\left(\frac{x}{10}\right) - T\left(\frac{x}{11}\right) - T\left(\frac{x}{13}\right) + T\left(\frac{x}{14}\right) + T\left(\frac{x}{15}\right) - T\left(\frac{x}{17}\right) - \ldots$$

Примѣръ 2. Дана функція

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \theta(\sqrt[4]{x}) + \ldots;$$

отсюда выводимъ

$$\theta(x) = A_1\psi(x) + A_2\psi(\sqrt{x}) + A_3\psi(\sqrt[3]{x}) + \ldots;$$

требуется опредѣлить коеффиціенты $A_1, A_2, A_3, \ldots$

Разсуждая подобно предыдущему, мы находимъ для $A_1, A_2, \ldots$ совершенно тѣ же значенія, что и въ предшествующей задачѣ. Слѣдовательно имѣемъ

$$\theta(x) = \psi(x) - \psi(\sqrt{x}) - \psi(\sqrt[3]{x}) - \psi(\sqrt[5]{x}) + \psi(\sqrt[6]{x}) - \ldots$$

Если $\psi(x)$ изображаетъ здѣсь ту же функцію, что и въ предыдущемъ примѣрѣ, то въ послѣднемъ равенствѣ можно подставить на мѣсто членовъ во второй части соотвѣтствующія имъ выраженія посредствомъ функціи $T(x)$, и написать

$$\begin{aligned}
\theta(x) = {} & T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) + T\left(\frac{x}{6}\right) - \ldots \\
& - T(\sqrt{x}) + T\left(\frac{\sqrt{x}}{2}\right) + T\left(\frac{\sqrt{x}}{3}\right) + T\left(\frac{\sqrt{x}}{5}\right) - T\left(\frac{\sqrt{x}}{6}\right) + \ldots \\
& - T(\sqrt[3]{x}) + T\left(\frac{\sqrt[3]{x}}{2}\right) + T\left(\frac{\sqrt[3]{x}}{3}\right) + T\left(\frac{\sqrt[3]{x}}{5}\right) - T\left(\frac{\sqrt[3]{x}}{6}\right) + \ldots \\
& - T(\sqrt[5]{x}) + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& + T(\sqrt[6]{x}) - \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& - \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Въ послѣднемъ равенствѣ подъ $\theta(x)$ и $T(x)$ можно, между прочимъ, понимать логариѳмъ произведенія всѣхъ простыхъ чиселъ, не превышающихъ x, и логариѳмъ произведенія всѣхъ цѣлыхъ чиселъ, не превышающихъ x.

ГЛАВА II.

Рѣшеніе въ цѣлыхъ числахъ нѣсколькихъ неопредѣленныхъ задачъ.

§ I. Общее рѣшеніе линейнаго однороднаго уравненія.

Выводъ теоремы.

16. **Теорема.** *Если* $a_1, a_2, \dots a_n$ *цѣлыя числа, не имѣющія общаго дѣлителя, то всѣ рѣшенія въ цѣлыхъ числахъ однороднаго уравненія*

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = 0$$

опредѣляются по формуламъ:

$$x_1 = a_1 t_{1,1} + a_2 t_{1,2} + \dots + a_n t_{1,n},$$
$$x_2 = a_1 t_{2,1} + a_2 t_{2,2} + \dots + a_n t_{2,n},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$x_n = a_1 t_{n,1} + a_2 t_{n,2} + \dots + a_n t_{n,n},$$

гдѣ $t_{1,1}, \dots t_{n,n}$ *изображаютъ цѣлыя перемѣнныя числа, изъ которыхъ*

$$t_{1,2}, t_{1,3}, \dots t_{1,n},$$
$$t_{2,3}, \dots t_{2,n},$$
$$\dots\dots$$
$$\dots$$
$$t_{n-1,n}$$

суть произвольныя, остальныя же выражаются такъ:

$$t_{i,j} = -t_{j,i}, \quad t_{i,i} = 0.$$

Теорема очевидна въ случаѣ $n = 2$.[x)] Чтобы доказать ея справедливость при всякомъ данномъ n, можно ввести предположеніе, что она уже доказана во всѣхъ случаяхъ, когда число неизвѣстныхъ меньше n. Этимъ мы воспользуемся для доказательства, что всякое рѣшеніе уравненія

$$(1) \ldots\ldots\ldots a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = 0$$

получается изъ формулъ, приведенныхъ въ теоремѣ.

1. Что всякая система чиселъ, опредѣляемая означенными формулами, дѣйствительно даетъ рѣшеніе уравненія (1), въ этомъ мы удостовѣряемся непосредственно, внося въ (1) на мѣсто $x_1, x_2, \ldots$ соотвѣтствующія выраженія и принимая въ соображеніе, что $t_{i,j} = -t_{j,i}$, $t_{i,i} = 0$.

Наоборотъ, Пусть дана будетъ какая нибудь система чиселъ $x_1, x_2, \ldots x_n$, представляющая рѣшеніе уравненія (1); возьмемъ во вниманіе одно изъ этихъ чиселъ, напримѣръ x_m, и найдемъ $n-1$ чиселъ $u_{1,m}, u_{2,m}, \ldots u_{m-1,m}, u_{m+1,m}, \ldots u_{n,m}$, удовлетворяющихъ уравненію

$$a_1 u_{1,m} + a_2 u_{2,m} + \ldots + a_{m-1} u_{m-1,m} + a_{m+1} u_{m+1,m} + \ldots$$
$$+ a_n u_{n,m} + x_m = 0.$$

Такія числа всегда существуютъ; ибо общій наибольшій дѣлитель коеффиціентовъ $a_1, a_2, \ldots a_{m-1}, a_{m+1}, \ldots a_n$, на основаніи (1), дѣлитъ x_m.[xx)]

Внося въ (1) на мѣсто x_m выраженіе, получаемое изъ послѣдняго уравненія, имѣемъ

$$a_1(x_1 - a_m u_{1,m}) + \ldots + a_{m-1}(x_{m-1} - a_m u_{m-1,m})$$
$$+ a_{m+1}(x_{m+1} - a_m u_{m+1,m}) + \ldots + a_n(x_n - a_m u_{n,m}) = 0.$$

x) При $n=2$ будетъ $a_1x_1+a_2x_2=0$ или $\frac{x_1}{x_2}=-\frac{a_2}{a_1}$, откуда $x_1=a_2t$, $x_2=-a_1t$.

xx) По условію, числа $a_1, a_2, \ldots, a_{m-1}, a_m, a_{m+1}, \ldots, a_n$ не имѣютъ общаго наибольшаго дѣлителя; значитъ, общій наибольшій [illegible] чиселъ $a_1, a_2, \ldots, a_{m-1}, a_{m+1}, \ldots$ [illegible] можетъ дѣлить число a_m [illegible]

Разсматривая это уравненіе, какъ однородное съ $n-1$ неизвѣстными, на основаніи сдѣланнаго выше предположенія, можно написать:

$$x_1 - a_m u_{1,m} = \frac{a_1}{d_m} u_{1,1} + \ldots + \frac{a_{m-1}}{d_m} u_{1,m-1} + \frac{a_{m+1}}{d_m} u_{1,m+1} + \ldots + \frac{a_n}{d_m} u_{1,n},$$

. . . .

. . . .

$$x_{m-1} - a_m u_{m-1,m} = \frac{a_1}{d_m} u_{m-1,1} + \ldots\ldots + \frac{a_n}{d_m} u_{m-1,n},$$

$$x_{m+1} - a_m u_{m+1,m} = \frac{a_1}{d_m} u_{m+1,1} + \ldots\ldots + \frac{a_n}{d_m} u_{m+1,n},$$

. . . .

. . . .

$$x_n - a_m u_{n,m} = \frac{a_1}{d_m} u_{n,1} + \ldots\ldots + \frac{a_n}{d_n} u_{n,n},$$

гдѣ d_m есть общій наибольшій дѣлитель чиселъ $a_1, a_2, \ldots a_{m-1}, a_{m+1}, \ldots a_n$; числа $u_{1,1}, u_{1,2}, \ldots$ связаны лишь условіями $u_{i,j} = -u_{j,i}$, $u_{i,i} = 0$, а въ остальныхъ отношеніяхъ суть произвольны.

Послѣднія уравненія, взятыя вмѣстѣ съ однимъ изъ предшествующихъ и будучи приведены въ надлежащій порядокъ, даютъ намъ слѣдующую систему:

$$(2)\quad \begin{cases} d_m x_1 = a_1 u_{1,1} + \ldots + a_m d_m u_{1,m} + \ldots + a_n u_{1,n}, \\ d_m x_2 = a_1 u_{2,1} + \ldots + a_m d_m u_{2,m} + \ldots + a_n u_{2,n}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ d_m x_m = a_1 d_m u_{m,1} + \ldots + a_m d_m u_{m,m} + \ldots + a_n d_m u_{m,n}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ d_m x_n = a_1 u_{n,1} + \ldots + a_m d_m u_{n,m} + \ldots + a_n u_{n,n}, \end{cases}$$

Здѣсь выраженіе страницы 43

$x_m = -a_1 \cdot u_{1,m} - a_2 \cdot u_{2,m} - \ldots - a_{m-1} \cdot u_{m-1,m} - a_{m+1} \cdot u_{m+1,m} - \ldots - a_n \cdot u_{n,m}$

замѣнено выраженіемъ

$x_m = a_1 \cdot u_{m,1} + a_2 \cdot u_{m,2} + \ldots + a_{m-1} \cdot u_{m,m-1} + a_m \cdot u_{m,m} + a_{m+1} \cdot u_{m,m+1} + \ldots + a_n$

въ [illegible] $u_{m,m} = 0$; $u_{m,1} = -u_{1,m}$; $u_{m,2} = -u_{2,m}$; и т. д. [illegible]

чительно для симметріи формулъ;
при чемъ опять замѣчаемъ, что коеффиціенты во вторыхъ частяхъ у буквъ $a_1, a_2, \ldots a_n$, расположенные по діагонали, равны нулю, а каждые два, симметрически расположенные относительно діагонали, равны по числовой величинѣ, но знаки ихъ противоположны.

Числа $d_1, d_2, \ldots d_n$ не имѣютъ общаго дѣлителя; поэтому мы можемъ найти числа $h_1, h_2, \ldots h_n$, удовлетворяющія уравненію

$$(3) \ldots\ldots\ldots h_1 d_1 + h_2 d_2 + \ldots + h_n d_n = 1.$$

Найдя ихъ, мы умножаемъ обѣ части каждаго изъ уравненій (2) на h_m и затѣмъ выписываемъ отдѣльно всѣ частныя системы (2), соотвѣтствующія значеніямъ $m = 1, 2, \ldots n$. Складывая почленно сперва первыя уравненія въ этихъ системахъ, затѣмъ вторыя и т. д., и принимая во вниманіе каждый разъ равенство (3), получаемъ новую систему слѣдующаго вида:

$$\begin{aligned} x_1 &= a_1 t_{1,1} + a_2 t_{1,2} + \ldots + a_n t_{1,n}, \\ x_2 &= a_1 t_{2,1} + a_2 t_{2,2} + \ldots + a_n t_{2,n}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= a_1 t_{n,1} + a_2 t_{n,2} + \ldots + a_n t_{n,n}, \end{aligned}$$

гдѣ $t_{1,1}, \ldots t_{n,n}$ суть цѣлыя числа, удовлетворяющія условіямъ

$$t_{i,j} = -t_{j,i}, \qquad t_{i,i} = 0.$$

Что и слѣдовало доказать.

17. Для приложенія только что доказанной теоремы покажемъ рѣшеніе слѣдующей задачи.

Задача. Найти шесть чиселъ $x_1, x_2, x_3, y_1, y_2, y_3$, которыя удовлетворяли бы тремъ такимъ условіямъ:

$$\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} = a_1, \quad \begin{vmatrix} x_1 & y_1 \\ x_3 & y_3 \end{vmatrix} = a_2, \quad \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = a_3,$$

(гдѣ a_1, a_2, a_3 изображаютъ данныя числа, не имѣющія общаго дѣлителя).

Изъ очевидныхъ равенствъ [illegible]

$$\begin{vmatrix} a_1 & x_1 & x_1 \\ a_2 & x_2 & x_2 \\ a_3 & x_3 & x_3 \end{vmatrix} = 0, \qquad \begin{vmatrix} a_1 & x_1 & y_1 \\ a_2 & x_2 & y_2 \\ a_3 & x_3 & y_3 \end{vmatrix} = 0$$

выводимъ [illegible]:

$$(1) \ldots\ldots \begin{cases} a_1 x_1 - a_2 x_2 + a_3 x_3 = 0, \\ a_1 y_1 - a_2 y_2 + a_3 y_3 = 0. \end{cases}$$

Слѣдовательно можно написать [illegible]

$$x_1 = a_1 t_{11} - a_2 t_{12} + a_3 t_{13},$$

$$x_2 = a_1 t_{21} - a_2 t_{22} + a_3 t_{23},$$

$$x_3 = a_1 t_{31} - a_2 t_{32} + a_3 t_{33};$$

здѣсь t_{12}, t_{13}, t_{23} изображаютъ новыя неизвѣстныя цѣлыя числа, введенныя на мѣсто x_1, x_2, x_3; кромѣ того имѣемъ $t_{ab} = -t_{ba}$, $t_{aa} = 0$.

Съ помощью послѣднихъ уравненій находимъ

$$[illegible] = \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} = a_1 - [illegible] = [illegible]$$

$$\begin{vmatrix} x_1 & y_1 \\ x_3 & y_3 \end{vmatrix} = a_2 - [illegible] = [illegible]$$

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = a_3 - [illegible] = [illegible]$$

Окончательное рѣшеніе получается слѣдующимъ образомъ:

Взявъ для y_1, y_2, y_3 какое угодно частное рѣшеніе втораго уравненія (1) и положивъ, что y_1, y_2, y_3 не имѣютъ общаго дѣлителя, мы дадимъ для неизвѣстныхъ $t_{1,2}$, $t_{1,3}$, $t_{2,3}$ значенія, удовлетворяющія условію

$$-y_3 t_{1,2} + y_2 t_{1,3} - y_1 t_{2,3} = 1;$$

Выбравъ такимъ образомъ любую изъ системъ чиселъ $t_{1,2}, t_{1,3}, t_{2,3}$, удовлетворяющую этому условію, мы по этимъ числамъ опредѣлимъ x_1, x_2 и x_3.

[redacted] предыдущія уравненія примутъ слѣдующій видъ: (при этомъ)

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = a_3, \quad \begin{vmatrix} x_1 & y_1 \\ x_3 & y_3 \end{vmatrix} = a_2, \quad \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} = a_1.$$

Это показываетъ, что числа x_1, x_2, x_3, y_1, y_2, y_3, полученныя по указанному способу, составляютъ рѣшеніе предложенной задачи.

Этотъ методъ можно обобщить, но мы не будемъ надъ нимъ останавливаться. Покажемъ лучше пріемъ для рѣшенія другой задачи въ подобномъ родѣ.

§ II. Составленіе опредѣлителя, значеніе котораго равно 1, при данныхъ элементахъ первой строки.

18. Совокупность n данныхъ чиселъ согласимся называть сочетаніемъ и изображать для сокращенія одной буквой

$$S = (a, a_1, a_2, \ldots a_{n-1}).$$

На знаки чиселъ и на порядокъ, въ которомъ они размѣщены, никакого вниманія обращать не будемъ; такъ что можно написать

$$(a, a_1, a_2, a_3) = (a_1, -a_2, -a, a_3) = (a_3, -a, a_1, -a_2).$$

Два сочетанія

$$S = (a, a_1, \ldots a_{n-1}),$$
$$T = (a, a'_1, \ldots a'_{n-1}),$$

состоящія изъ одинаковаго числа элементовъ, въ которыхъ по крайней мѣрѣ одинъ элементъ, напримѣръ a, общій, а остальные, соотвѣтственные одинъ другому, отличаются кратностью a, называть будемъ смежными. Напримѣръ, два сочетанія $(3, 5, -7)$ и $(3, 1, 2)$ смежны, ибо $5 = 2 + 3$ и $7 = 1 + 2 . 3$.

Въ двухъ смежныхъ сочетаніяхъ общіе наибольшіе дѣлители составляющихъ элементовъ равны между собою.

Каковы бы ни были два смежныхъ сочетанія

$$S = (a, a_1, \ldots a_{n-1}) .$$
$$T = (b, b_1, \ldots b_{n-1}),$$

всякій опредѣлитель

$$\Delta = \begin{vmatrix} b & b_1 & b_2 & \ldots & b_{n-1} \\ b' & b'_1 & b'_2 & \ldots & b'_{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ b^{(n-1)} & b_1^{(n-1)} & b_2^{(n-1)} & \ldots & b_{n-1}^{(n-1)} \end{vmatrix},$$

въ которомъ элементы первой строки совпадаютъ съ элементами сочетанія T, можетъ быть преобразованъ такъ, что элементы первой строки будутъ совпадать съ элементами сочетанія S. Предложеніе это вытекаетъ изъ основныхъ свойствъ опредѣлителя, по которымъ элементы первой строки можно привести въ какой угодно порядокъ, можно произвольно мѣнять знаки у этихъ же элементовъ и, наконецъ, къ любому изъ элементовъ $b_0, b_1, b_2, \ldots b_{n-1}$ можно прибавить или вычесть произвольную кратность какого нибудь изъ остальныхъ; при этомъ приходится каждый разъ производить надлежащія измѣненія надъ прочими элементами опредѣлителя.

19. Принимая во вниманіе все вышесказанное легко показать, какъ найти рѣшеніе въ цѣлыхъ числахъ уравненія

Способъ рѣшенія задачи.

$$\begin{vmatrix} a & a_1 & a_2 \ldots a_{n-1} \\ x & x_1 & x_2 \ldots x_{n-1} \\ y & y_1 & y_2 \ldots y_{n-1} \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ z & z_1 & z_2 \ldots z_{n-1} \end{vmatrix} = 1,$$

въ которомъ a, $a_1, \ldots a_{n-1}$ суть данныя числа, не имѣющія общаго дѣлителя.

Для этого мы принимаемъ во вниманіе сочетаніе

$$S = (a, a_1, \ldots a_{n-1}),$$

и отмѣчая въ немъ самый малый по числовой величинѣ элементъ a_i, не равный нулю, замѣняемъ всѣ остальные элементы ихъ остатками отъ дѣленія на a_i; такимъ образомъ получаемъ новое сочетаніе

$$S_1 = (b, b_1, \ldots b_{n-1}),$$

смежное съ предыдущимъ, съ элементами меньшими по числовой величинѣ: наибольшій элементъ въ S_1 равенъ наименьшему въ S. Теперь повторяемъ подобную операцію съ элементами сочетанія S_1, то есть, отмѣтивъ наименьшій элементъ b_i, замѣняемъ всѣ остальные элементы въ S_1 ихъ остатками отъ дѣленія на b_i; получаемъ новое сочетаніе

$$S_2 = (c, c_1, \ldots c_{n-1}),$$

смежное съ S_1, но съ элементами меньшими чѣмъ въ S_1. Подобнымъ образомъ продолжаемъ дѣйствовать до тѣхъ поръ, пока не дойдемъ до сочетанія S_r, всѣ элементы котораго будутъ рав-

ными нулю, за исключеніемъ одного, равнаго 1; общій наибольшій дѣлитель элементовъ каждаго изъ сочетаній $S_1, S_2, \ldots$ будетъ равняться 1.

Какъ только составленъ нами рядъ сочетаній

$$(1) \ldots\ldots\ldots\ldots S, S_1, S_2, \ldots S_{r-1}, S_r,$$

переходимъ къ составленію опредѣлителя вида

$$\Delta_r = \begin{vmatrix} 1 & 0 & 0 \ldots 0 \\ p & p_1 & p_2 \ldots p_{n-1} \\ q & q_1 & q_2 \ldots q_{n-1} \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ r & r_1 & r_2 \ldots r_{n-1} \end{vmatrix}$$

съ цѣлыми элементами, значеніе котораго равнялось бы 1. Достигнуть этого очень легко разными способами: можно, напримѣръ, приравнять 1 всѣ элементы на діагонали и нулю всѣ элементы надъ діагональю, оставивъ произвольными тѣ элементы, которые расположены подъ діагональю.

Такъ какъ элементы первой строки въ Δ_r представляютъ сочетаніе S_r, то опредѣлитель этотъ можно преобразовать въ другой, въ которомъ элементы первой строки представятъ сочетаніе S_{r-1}. Обозначивъ этотъ новый опредѣлитель чрезъ Δ_{r-1}, мы замѣчаемъ, что въ свою очередь его легко преобразовать въ другой Δ_{r-2}, первая строка котораго представитъ сочетаніе S_{r-2}. Продолжая такимъ образомъ преобразовывать вновь получаемые опредѣлители, мы дойдемъ наконецъ до опредѣлителя Δ, въ которомъ элементы первой строки будутъ представлять сочетаніе S, и будемъ имѣть равенства

$$\Delta = \Delta_1 = \Delta_2 = \ldots = \Delta_r;$$

а такъ какъ по предположенію $\Delta_r = 1$, то слѣдовательно

$$\Delta = 1.$$

Это показываетъ, что элементы опредѣлителя Δ, содержащіе $\frac{n(n-1)}{2}$ произвольныхъ цѣлыхъ перемѣнныхъ, даютъ безчисленное множество рѣшеній предложенной задачи.

20. *Примѣръ*. Требуется составить опредѣлитель четвертаго порядка, въ которомъ первая строка состояла бы изъ элементовъ 3, 5, 8, 7, и значеніе котораго равнялось бы 1. Примѣръ.

Составляемъ рядъ сочетаній

$$S = (3,\ 5,\ 8,\ 7),\quad S_1 = (3,\ 2,\ -1,\ 1),\quad S_2 = (0,\ 0,\ 0,\ 1),$$

а съ ихъ помощью получается соотвѣтствующій рядъ опредѣлителей

$$\Delta_2 = \begin{vmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \\ y & y_1 & 1 & 0 \\ z & z_1 & z_2 & 1 \end{vmatrix},\quad \Delta_1 = \begin{vmatrix} 1 & -1 & 2 & 3 \\ x & 1-x & 2x & 3x \\ y & y_1 - y & 1+2y & 3y \\ z & z_1 - z & z_2 + 2z & 1+3z \end{vmatrix},$$

$$\Delta = \begin{vmatrix} 7 & 8 & 5 & 3 \\ 7x & 1+8x & 5x & 3x \\ 7y & y_1 + 8y & 1+5y & 3y \\ 2+7z & 3+8z+z_1 & 1+5z+z_2 & 1+3z \end{vmatrix}.$$

Всѣ они равны 1; поэтому послѣдній удовлетворяетъ всѣмъ требованіямъ задачи.

§ III. Составленіе опредѣлителя при другихъ условіяхъ.

Предварительныя замѣчанія и способъ изъясненія задачи.

22. Возьмемъ теперь во вниманіе двойное сочетаніе, состоящее изъ $2n$ чиселъ, выписанныхъ въ извѣстномъ порядкѣ въ двухъ строкахъ, по n чиселъ въ каждой,

$$S = \begin{pmatrix} a, a_1, a_2, \ldots a_{n-1} \\ b, b_1, b_2, \ldots b_{n-1} \end{pmatrix}.$$

Два сочетанія подобнаго рода, которыя отличаются только порядкомъ столбцовъ, согласимся разсматривать какъ тожественныя; также одновременное измѣненіе знаковъ у обоихъ элементовъ какого либо столбца не будемъ считать за нарушеніе сочетанія. На этомъ основаніи можно написать

$$\begin{pmatrix} a, a_1, a_2 \\ b, b_1, b_2 \end{pmatrix} = \begin{pmatrix} a_2, -a, a_1 \\ b_2, -b, b_1 \end{pmatrix}.$$

Въ данномъ двойномъ сочетаніи отмѣтимъ какой нибудь столбецъ, и затѣмъ къ элементамъ каждаго изъ остальныхъ столбцовъ прибавимъ или вычтемъ соотвѣтственно элементы отмѣченнаго нами столбца, умноженные на какое угодно цѣлое число. Полученное такимъ образомъ новое двойное сочетаніе будемъ называть смежнымъ съ предыдущимъ. Такъ, напримѣръ, два сочетанія

$$\begin{pmatrix} a, a_1, a_2 \\ b, b_1, b_2 \end{pmatrix}, \quad \begin{pmatrix} a + ka_1, a_1, a_2 + la_1 \\ b + kb_1, b_1, b_2 + lb_1 \end{pmatrix}$$

суть смежныя.

Легко показать, что если два сочетанія

$$\begin{pmatrix} a, a_1, a_2, \ldots a_{n-1} \\ b, b_1, b_2, \ldots b_{n-1} \end{pmatrix} \text{ и } \begin{pmatrix} a', a'_1, a'_2, \ldots a'_{n-1} \\ b', b'_1, b'_2, \ldots b'_{n-1} \end{pmatrix}$$

суть смежныя, то общій наибольшій дѣлитель чиселъ

$$ab_1 - a_1b,\ ab_2 - a_2b, \ldots a_{n-1}b_n - a_nb_{n-1}$$

равенъ общему наибольшему дѣлителю чиселъ

$$a'b'_1 - a'_1b',\ a'b'_2 - a'_2b', \ldots a'_{n-1}b'_n - a'_nb'_{n-1}.$$

Дѣйствуя подобно тому, какъ было показано въ предшествующемъ номерѣ, можно для всякаго двойнаго сочетанія S составить рядъ сочетаній

$$S,\ S_1,\ S_2, \ldots S_r,$$

въ которомъ каждое слѣдующее будетъ смежнымъ съ предшествующимъ, а послѣднее будетъ вида

$$S_r = \begin{pmatrix} c, & 0, & 0, \ldots 0 \\ d, & d', & 0, \ldots 0 \end{pmatrix},$$

при чемъ произведеніе cd' будетъ равняться общему наибольшему дѣлителю опредѣлителей $ab_1 - a_1b,\ ab_2 - a_2b, \ldots,$ составленныхъ изъ элементовъ сочетанія S.

Съ другой стороны ясно, что всякій опредѣлитель n-го порядка съ цѣлыми элементами, въ которомъ двѣ первыя строки представляютъ собой двойное сочетаніе S_i, можно преобразовать въ другой, въ которомъ двѣ первыя строки представятъ сочетаніе S_{i-1}, смежное съ предыдущимъ. Это даетъ возможность составлять рѣшенія въ цѣлыхъ числахъ такого неопредѣленнаго уравненія:

$$\begin{vmatrix} a & a_1 & a_2 \ldots a_{n-1} \\ b & b_1 & b_2 \ldots b_{n-1} \\ x & x_1 & x_2 \ldots x_{n-1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ z & z_1 & z_2 \ldots z_{n-1} \end{vmatrix} = h,$$

гдѣ h есть общій наибольшій дѣлитель чиселъ $ab_1 - a_1b$, $ab_2 - a_2b, \ldots$

Въ самомъ дѣлѣ, обозначивъ чрезъ S двойное сочетаніе, представляемое двумя первыми строками послѣдняго опредѣлителя, и выписавъ рядъ смежныхъ сочетаній

$$S, S_1, S_2, \ldots S_{r-1}, S_r,$$

гдѣ

$$S_r = \begin{pmatrix} c, 0, & 0, \ldots 0 \\ d, d', & 0, \ldots 0 \end{pmatrix}, \quad cd' = h,$$

составимъ опредѣлитель Δ_r съ цѣлыми элементами, котораго значеніе равнялось бы h, а первыя двѣ строки представляли сочетаніе S_r; такому требованію удовлетворяетъ опредѣлитель

$$\Delta_r = \begin{vmatrix} c & 0 & 0 \ldots 0 \\ d & d' & 0 \ldots 0 \\ p & p_1 & 1 \ldots 0 \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ r & r_1 & r_2 \ldots 1 \end{vmatrix},$$

въ которомъ $p, p_1, \ldots r_{n-1}$ изображаютъ произвольныя цѣлыя числа.

Опредѣлитель Δ_r преобразовываемъ въ Δ_{r-1}, этотъ послѣдній въ Δ_{r-2}, этотъ въ свою очередь въ Δ_{r-3} и такъ далѣе, — такимъ именно образомъ, чтобы первыя двѣ строки въ каждомъ опредѣлителѣ Δ_i представляли собой сочетаніе S_i. Поступая такъ, дойдемъ въ концѣ до опредѣлителя Δ, выраженіе котораго дастъ намъ безконечное множество частныхъ рѣшеній заданнаго уравненія.

22. *Примѣръ. Найти опредѣлитель четвертаго порядка, значеніе котораго равнялось бы* 1, *и чтобъ первыя двѣ строки были слѣдующія:* Примѣръ.

$$\begin{matrix} 2 & 3 & 5 & 7, \\ 3 & 4 & -1 & 0. \end{matrix}$$

Составляемъ рядъ сочетаній

$$S=\begin{pmatrix} 2 & 3 & 5 & 7 \\ 3 & 4 & -1 & 0 \end{pmatrix}, \quad S_1=\begin{pmatrix} 2 & 1 & 1 & 1 \\ 3 & 1 & -7 & -9 \end{pmatrix},$$

$$S_2=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & -8 & -10 \end{pmatrix}, \quad S_3=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Соотвѣтственно этому имѣемъ

$$\Delta_3=\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ x & x_1 & 1 & 0 \\ y & y_1 & y_2 & 1 \end{vmatrix}, \quad \Delta_2=\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & -8 & -10 \\ x & x_1 & 1-8x_1 & -10x_1 \\ y & y_1 & y_2-8y_1 & 1-10y_1 \end{vmatrix},$$

$$\Delta_1=\begin{vmatrix} 1 & 2 & 1 & 1 \\ 1 & 3 & -7 & -9 \\ x & 2x+x_1 & 1+x-8x_1 & x-10x_1 \\ y & 2y+y_1 & y-8y_1+y_2 & 1+y-10y_1 \end{vmatrix},$$

$$\Delta=\begin{vmatrix} 3 & 2 & 5 & 7 \\ 4 & 3 & -1 & 0 \\ 3x+x_1 & 2x+x_1 & 1+5x-6x_1 & 7x-7x_1 \\ 3y+y_1 & 2y+y_1 & 5y-6y_1+y_2 & 1+7y-7y_1 \end{vmatrix}.$$

Послѣдній опредѣлитель удовлетворяетъ требуемымъ условіямъ при всякихъ цѣлыхъ значеніяхъ для x, y, x_1, y_1, y_2.

§ IV. Новое рѣшеніе предыдущей задачи въ частномъ случаѣ, когда опредѣлитель четвертаго порядка.

Рѣшеніе вспомогательной задачи.

23. Задача, занимающая насъ въ предшествующемъ номерѣ, имѣетъ особенное примѣненіе въ теоріи квадратичныхъ формъ; преимущественно частный случай, когда опредѣлитель есть четвертаго порядка. Только что изложенный способъ нахожденія рѣшеній хотя и хорошъ въ практическомъ отношеніи, когда данные элементы выражены числами, но представляется неудобнымъ, если желаемъ дѣлать теоретическія заключенія на счетъ искомыхъ чиселъ. Поэтому-то мы изложимъ здѣсь иной способъ рѣшенія, основанный на другихъ началахъ. Но прежде всего займемся рѣшеніемъ слѣдующей вспомогательной задачи.

Даны шесть цѣлыхъ чиселъ $a_{0,1}$, $a_{0,2}$, $a_{0,3}$, $a_{1,2}$, $a_{1,3}$, $a_{2,3}$, *удовлетворяющихъ условію*

$$a_{0,1}\,a_{2,3} - a_{0,2}\,a_{1,3} + a_{0,3}\,a_{1,2} = 0,$$

требуется найти восемь цѣлыхъ чиселъ

$$p,\ p_1,\ p_2,\ p_3,$$

$$q,\ q_1,\ q_2,\ q_3,$$

которыя удовлетворяли бы слѣдующимъ шести уравненіямъ:

$$\begin{vmatrix} p & q \\ p_1 & q_1 \end{vmatrix} = a_{0,1},\quad \begin{vmatrix} p & q \\ p_2 & q_2 \end{vmatrix} = a_{0,2},\quad \begin{vmatrix} p & q \\ p_3 & q_3 \end{vmatrix} = a_{0,3},$$

$$\begin{vmatrix} p_1 & q_1 \\ p_2 & q_2 \end{vmatrix} = a_{1,2},\quad \begin{vmatrix} p_1 & q_1 \\ p_3 & q_3 \end{vmatrix} = a_{1,3},\quad \begin{vmatrix} p_2 & q_2 \\ p_3 & q_3 \end{vmatrix} = a_{2,3}.$$

Очевидно, можно ограничиться предположеніемъ, что числа $a_{0,1}, a_{0,2}, \ldots a_{2,3}$ не имѣютъ общаго дѣлителя.

Чтобы придать формуламъ болѣе симметричный видъ, введемъ новыя обозначенія

$$a_{1,0} = -a_{0,1},\ a_{2,0} = -a_{0,2}, \ldots,$$
$$a_{0,0} = 0, \qquad a_{1,1} = 0, \ldots;$$

такъ что, вообще, имѣемъ

$$a_{i,j} = -a_{j,i},\ a_{i,i} = 0.$$

Изъ условныхъ уравненій, которымъ должны удовлетворять числа $p, q, p_1, q_1, \ldots$ вытекаетъ непосредственно слѣдующая группа уравненій:

$$(1) \ldots\ldots \begin{cases} a_{1,2}p + a_{2,0}p_1 + a_{0,1}p_2 + \quad 0 \quad = 0, \\ a_{1,3}p + a_{3,0}p_1 + \quad 0 \quad + a_{0,1}p_3 = 0, \\ a_{2,3}p + \quad 0 \quad + a_{3,0}p_2 + a_{0,2}p_3 = 0, \\ \quad 0 \quad + a_{2,3}p_1 + a_{3,1}p_2 + a_{1,2}p_3 = 0, \end{cases}$$

и точно такимъ же уравненіямъ должны удовлетворять q, q_1, q_2, q_3.

Не всѣ уравненія (1) независимы другъ отъ друга: легко замѣтить, что два какія нибудь выводятся изъ двухъ остальныхъ простымъ исключеніемъ одного неизвѣстнаго; при этомъ слѣдуетъ имѣть въ виду предположенную зависимость между $a_{0,1}, a_{0,2}, \ldots a_{2,3}$. Поэтому уравненія (1) имѣютъ безчисленное множество рѣшеній въ цѣлыхъ числахъ, и не трудно доказать, что всѣ они получаются изъ формулъ

$$(2) \ldots\ldots \begin{cases} p = a_{0,0}t + a_{0,1}t_1 + a_{0,2}t_2 + a_{0,3}t_3, \\ p_1 = a_{1,0}t + a_{1,1}t_1 + a_{1,2}t_2 + a_{1,3}t_3, \\ p_2 = a_{2,0}t + a_{2,1}t_1 + a_{2,2}t_2 + a_{2,3}t_3, \\ p_3 = a_{3,0}t + a_{3,1}t_1 + a_{3,2}t_2 + a_{3,3}t_3, \end{cases}$$

гдѣ t, t_1, t_2, t_3 суть произвольныя цѣлыя числа.

Въ самомъ дѣлѣ, внося въ (1) на мѣсто p, p_1, p_2, p_3 соотвѣтствующія выраженія по формуламъ (2), мы замѣчаемъ, что въ результатѣ получаются тожества; остается слѣдовательно удостовѣриться, что всякое рѣшеніе уравненій (1) можетъ быть получено изъ (2) при нѣкоторыхъ частныхъ значеніяхъ для t, t_1, t_2, t_3.

Изображая чрезъ d_3 общій наибольшій дѣлитель трехъ чиселъ $a_{0,1}, a_{0,2}, a_{1,2}$ и принимая во вниманіе первое уравненіе (1), имѣемъ

$$(3)\dots\dots\quad \begin{cases} d_3 p = a_{0,0} u + a_{0,1} u_1 + a_{0,2} u_2, \\ d_3 p_1 = a_{1,0} u + a_{1,1} u_1 + a_{1,2} u_2, \\ d_3 p_2 = a_{2,0} u + a_{2,1} u_1 + a_{2,2} u_2, \end{cases}$$

гдѣ u, u_1, u_2 изображаютъ цѣлыя числа.

Внося во второе уравненіе (1) на мѣсто p и p_1 соотвѣтствующія выраженія по послѣднимъ формуламъ, получаемъ

$$a_{1,0} a_{3,0} u + a_{0,1} a_{1,3} u_1 + a_{0,1} a_{2,3} u_2 + a_{0,1} d_3 p_3 = 0;$$

отсюда, сокращая на $a_{0,1}$, выводимъ

$$(4)\dots\dots\dots\quad d_3 p_3 = a_{3,0} u + a_{3,1} u_1 + a_{3,2} u_2.$$

Слѣдовательно число p_3 выражается точно такимъ же образомъ какъ и p, p_1, p_2. Уравненіе (4) слѣдуетъ считать дополненіемъ къ (3). При выводѣ послѣдняго уравненія мы предполагали, что $a_{0,1}$ не равно нулю. Въ противномъ случаѣ слѣдовало бы выводить (4) не съ помощью втораго уравненія (1), а третьяго или четвертаго.

Если всѣ три числа $a_{0,1}, a_{0,2}, a_{1,2}$ равны нулю, дѣлитель d_3 становится неопредѣленнымъ, и вся группа (3), (4) должна быть оставлена безъ вниманія.

Подобно тому, какъ выведены были уравненія (3), (4), можно еще вывести нижеслѣдующія три группы, дающія новыя выраженія для тѣхъ же чиселъ p, p_1, p_2, p_3.

$$(5) \ldots\ldots \begin{cases} d_2 p = a_{0,0} u' + a_{0,1} u'_1 + a_{0,3} u'_3, \\ d_2 p_1 = a_{1,0} u' + a_{1,1} u'_1 + a_{1,3} u'_3, \\ d_2 p_2 = a_{2,0} u' + a_{2,1} u'_1 + a_{2,3} u'_3, \\ d_2 p_3 = a_{3,0} u' + a_{3,1} u'_1 + a_{3,3} u'_3; \end{cases}$$

$$(6) \ldots\ldots \begin{cases} d_1 p = a_{0,0} u'' + a_{0,2} u''_2 + a_{0,3} u''_3, \\ d_1 p_1 = a_{1,0} u'' + a_{1,2} u''_2 + a_{1,3} u''_3, \\ d_1 p_2 = a_{2,0} u'' + a_{2,2} u''_2 + a_{2,3} u''_3, \\ d_1 p_3 = a_{3,0} u'' + a_{3,2} u''_2 + a_{3,3} u''_3; \end{cases}$$

$$(7) \ldots\ldots \begin{cases} dp = a_{0,1} u'''_1 + a_{0,2} u'''_2 + a_{0,3} u'''_3, \\ dp_1 = a_{1,1} u'''_1 + a_{1,2} u'''_2 + a_{1,3} u'''_3, \\ dp_2 = a_{2,1} u'''_1 + a_{2,2} u'''_2 + a_{2,3} u'''_3, \\ dp_3 = a_{3,1} u'''_1 + a_{3,2} u'''_2 + a_{3,3} u'''_3; \end{cases}$$

гдѣ d_2 изображаетъ общій наибольшій дѣлитель чиселъ $a_{0,1}$, $a_{1,3}$, $a_{0,3}$; d_1 — чиселъ $a_{0,2}$, $a_{0,3}$, $a_{2,3}$; d — чиселъ $a_{1,2}$, $a_{1,3}$, $a_{2,3}$; буквы u', $u'_1 \ldots u'''_3$ изображаютъ цѣлыя числа.

Такъ какъ общій наибольшій дѣлитель чиселъ $a_{0,1}, a_{0,2}, \ldots a_{2,3}$ равенъ 1, то и общій наибольшій дѣлитель чиселъ d, d_1, d_2, d_3 также равенъ 1; поэтому можно найти четыре цѣлыхъ числа λ, λ_1, λ_2, λ_3, удовлетворяющихъ уравненію

$$d\lambda + d_1 \lambda_1 + d_2 \lambda_2 + d_3 \lambda_3 = 1.$$

Умножая обѣ части каждаго изъ уравненій (3) и (4) на λ_3, каждаго изъ уравненій (5) на λ_2 и т. д., затѣмъ складывая почленно первыя, вторыя, третія и четвертыя уравненія въ четырехъ означенныхъ группахъ, и полагая еще для сокращенія

$$\begin{aligned} t &= \lambda_3 u + \lambda_2 u' + \lambda_1 u'' + 0, \\ t_1 &= \lambda_3 u_1 + \lambda_2 u'_1 + 0 + \lambda u'''_1, \\ t_2 &= \lambda_3 u_2 + 0 + \lambda_1 u''_2 + \lambda u'''_2, \\ t_3 &= 0 + \lambda_2 u'_3 + \lambda_1 u''_3 + \lambda u'''_3, \end{aligned}$$

получаемъ группу (2), которая, слѣдовательно, выражаетъ всѣ рѣшенія въ цѣлыхъ числахъ уравненій (1).

Остается теперь показать, какія частныя значенія слѣдуетъ давать въ (2) для t, t_1, t_2, t_3, чтобы соотвѣтствующія имъ значенія p, p_1, p_2, p_3 и q, q_1, q_2, q_3 удовлетворяли заданнымъ уравненіямъ.

Подставивъ въ (2) на мѣсто t, t_1, t_2, t_3 какія угодно частныя цѣлыя значенія, вычислимъ соотвѣтствующія имъ значенія p', p'_1, p'_2, p'_3 и называя чрезъ l общій наибольшій дѣлитель этихъ послѣднихъ, положимъ

$$\frac{p'}{l}=q,\quad \frac{p'_1}{l}=q_1,\quad \frac{p'_2}{l}=q_2,\quad \frac{p'_3}{l}=q_3.$$

Числа q, q_1, q_2, q_3 очевидно удовлетворяютъ (1); принимая это въ соображеніе, изъ (2) выводимъ рядъ формулъ, которыя можно написать такъ:

$$p_i q_j - p_j q_i = a_{i,j}\,(qt + q_1 t_1 + q_2 t_2 + q_3 t_3),$$
$$\begin{pmatrix} i=0,\ 1,\ 2,\ 3 \\ j=0,\ 1,\ 2,\ 3 \end{pmatrix}.$$

Отсюда слѣдуетъ, что для значеній t, t_1, t_2, t_3, удовлетворяющихъ уравненію

$$qt + q_1 t_1 + q_2 t_2 + q_3 t_3 = 1,$$

будемъ имѣть

$$p_i q_j - p_j q_i = a_{i,j}$$

при всякихъ i и j. Такимъ образомъ задача наша рѣшена.

Рѣшеніе главнаго вопроса.

24. Переходимъ теперь къ рѣшенію главнаго нашего вопроса, именно, какъ найти цѣлыя числа u, u_1, . . . v_3, удовлетворяющія уравненію

$$(1)\ldots\ldots\ldots\ldots \begin{vmatrix} a & a_1 & a_2 & a_3 \\ b & b_1 & b_2 & b_3 \\ u & u_1 & u_2 & u_3 \\ v & v_1 & v_2 & v_3 \end{vmatrix} = h,$$

гдѣ h есть общій наибольшій дѣлитель шести чиселъ, именно:

$$ab_1 - a_1 b = ha_{2,3}, \quad ab_2 - a_2 b = ha_{1,3}, \quad ab_3 - a_3 b = ha_{1,2},$$
$$a_1 b_2 - a_2 b_1 = ha_{0,3}, \quad a_1 b_3 - a_3 b_1 = ha_{0,2}, \quad a_2 b_3 - a_3 b_2 = ha_{0,1}.$$

Для этого мы ищемъ прежде всего чиселъ p, p_1, p_2, p_3, q, q_1, q_2, q_3, которыя удовлетворяли бы такимъ условіямъ:

$$(2) \ldots \begin{cases} pq_1 - p_1 q = a_{0,1}, & pq_2 - p_2 q = -a_{0,2}, \\ pq_3 - p_3 q = a_{0,3}, & p_1 q_2 - p_2 q_1 = a_{1,2}, \\ p_1 q_3 - p_3 q_1 = -a_{1,3}, & p_2 q_3 - p_3 q_2 = a_{2,3}; \end{cases}$$

это возможно, ибо между числами $a_{0,1}, \ldots a_{2,3}$ имѣетъ мѣсто зависимость

$$a_{0,1} a_{2,3} - a_{0,2} a_{1,3} + a_{1,2} a_{0,3} = 0.$$

Съ другой стороны, уравненіе (1) можно написать такъ:

$$\begin{vmatrix} a & a_1 \\ b & b_1 \end{vmatrix} \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix} - \begin{vmatrix} a & a_2 \\ b & b_2 \end{vmatrix} \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix} + \begin{vmatrix} a & a_3 \\ b & b_3 \end{vmatrix} \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}$$
$$+ \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \begin{vmatrix} u & u_3 \\ v & v_3 \end{vmatrix} - \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \begin{vmatrix} u & u_2 \\ v & v_2 \end{vmatrix} + \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} \begin{vmatrix} u & u_1 \\ v & v_1 \end{vmatrix} = h,$$

а это, на основаніи принятыхъ выше обозначеній, приводится къ слѣдующему:

$$\begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix} \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix} + \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix} \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix} + \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix} \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}$$
$$+ \begin{vmatrix} p & p_3 \\ q & q_3 \end{vmatrix} \begin{vmatrix} u & u_3 \\ v & v_3 \end{vmatrix} + \begin{vmatrix} p & p_2 \\ q & q_2 \end{vmatrix} \begin{vmatrix} u & u_2 \\ v & v_2 \end{vmatrix} + \begin{vmatrix} p & p_1 \\ q & q_1 \end{vmatrix} \begin{vmatrix} u & u_1 \\ v & v_1 \end{vmatrix} = 1,$$

что, въ свою очередь, можетъ быть написано такъ:

$$(3)\quad \begin{vmatrix} pu + p_1 u_1 + p_2 u_2 + p_3 u_3 & qu + q_1 u_1 + q_2 u_2 + q_3 u_3 \\ pv + p_1 v_1 + p_2 v_2 + p_3 v_3 & qv + q_1 v_1 + q_2 v_2 + q_3 v_3 \end{vmatrix} = 1.$$

Чтобы найти цѣлыя числа $u, u_1, \ldots v_3$, удовлетворяющія послѣднему уравненію, принимаемъ во вниманіе формулы, опредѣляющія числа p, p_1, p_2, p_3, именно:

$$\begin{aligned} p &= 0 + a_{0,1} t_1 - a_{0,2} t_2 + a_{0,3} t_3, \\ p_1 &= -a_{0,1} t_1 + 0 + a_{1,2} t_2 - a_{1,3} t_3, \\ p_2 &= a_{0,2} t - a_{1,2} t_1 + 0 + a_{2,3} t_3, \\ p_3 &= -a_{0,3} t + a_{1,3} t_1 - a_{2,3} t_2 + 0\ , \end{aligned}$$

гдѣ t, t_1, t_2, t_3 суть числа цѣлыя, удовлетворяющія условію

$$qt + q_1 t_1 + q_2 t_2 + q_3 t_3 = 1,$$

и разсматривая эти числа, какъ извѣстныя, дадимъ для четырехъ неизвѣстныхъ v, v_1, v_2, v_3 такія значенія:

$$(4) \ldots\ldots\ v = t,\ v_1 = t_1,\ v_2 = t_2,\ v_3 = t_3;$$

тогда будемъ имѣть два уравненія

$$(5) \ldots\ldots \begin{cases} qv + q_1 v_1 + q_2 v_2 + q_3 v_3 = 1 \\ pv + p_1 v_1 + p_2 v_2 + p_3 v_3 = 0, \end{cases}$$

вслѣдствіе чего уравненіе (3), служащее для опредѣленія остальныхъ четырехъ неизвѣстныхъ u, u_1, u_2, u_3, принимаетъ видъ

$$\begin{vmatrix} pu + p_1 u_1 + p_2 u_2 + p_3 u_3 & qu + q_1 u_1 + q_2 u_2 + q_3 u_3 \\ 0 & 1 \end{vmatrix} = 1,$$

или

$$(6) \ldots\ldots\ pu + p_1 u_1 + p_2 u_2 + p_3 u_3 = 1.$$

Такъ какъ числа $a_{0,1}, a_{0,2}, \ldots a_{2,3}$ не имѣютъ общаго дѣлителя, то и числа p, p_1, p_2, p_3 также не имѣютъ общаго дѣлителя; это прямо видно изъ (2). Поэтому уравненіе (6) имѣетъ безчисленоое множество рѣшеній въ цѣлыхъ числахъ, и каждое изъ нихъ вмѣстѣ съ вышеопредѣленными числами v, v_1, v_2, v_3 даетъ рѣшеніе уравненія (1).

Между рѣшеніями уравненія (6) заслуживаютъ особаго вниманія тѣ, которыя удовлетворяютъ еще условію

$$\textbf{(7)} \ldots\ldots\ldots qu + q_1 u_1 + q_2 u_2 + q_3 u_3 = 0;$$

тогда (6) и (7) представятъ симметрическое соотвѣтствіе съ (5).

Что касается нахожденія цѣлыхъ рѣшеній уравненій (6) и (7), то вотъ къ чему оно приводится.

Изъ (7) выводимъ

$$\textbf{(8)} \ldots\ldots \begin{cases} u = \ \ 0 + q_1 x_1 + q_2 x_2 + q_3 x_3, \\ u_1 = -q x_1 + 0 + q_2 x_4 + q_3 x_5, \\ u_2 = -q x_2 - q_1 x_4 + 0 + q_3 x_6, \\ u_3 = -q x_3 - q_1 x_5 - q_2 x_6 + 0 \ , \end{cases}$$

гдѣ $x_1, \ldots x_6$ изображаютъ новыя неизвѣстныя. Внося въ (6) на мѣсто u, u_1, u_2, u_3 послѣднія выраженія, получаемъ

$$\textbf{(9)} \ a_{0,1} x_1 - a_{0,2} x_2 + a_{0,3} x_3 + a_{1,2} x_4 - a_{1,3} x_5 + a_{2,3} x_6 = 1.$$

Каждое рѣшеніе въ цѣлыхъ числахъ этого уравненія опредѣляетъ по (8) требуемую систему чиселъ u, u_1, u_2, u_3.

ГЛАВА III.

Понятіе о сравненіяхъ. — Теоремы Фермата, Эйлера и Вильсона. — Сравненія первой степени.

§ I. О сравненіяхъ вообще.

Общія свойства сравненій.

25. Если разность двухъ чиселъ a и b дѣлится на k, то говорятъ, что числа a и b *сравнимы* по *модулю* k, и это свойство изображаютъ такъ:

$$a \equiv b \text{ (mod. } k).$$

Сравниваемыя числа a и b могутъ быть съ какими угодно знаками, но модуль предполагается положительнымъ и >1. Число b называется вычетомъ числа a, или, наоборотъ, a есть вычетъ числа b.

Изъ опредѣленія сравненія непосредственно вытекаютъ нѣкоторыя его свойства, напоминающія основныя свойства уравненій, а именно:

1°. *Всякое число a сравнимо съ самимъ собою, то есть* $a \equiv a$ (mod. k). $a-a=0\cdot t$

2°. *Два числа, сравнимыя съ третьимъ по какому либо модулю, сравнимы между собою по тому же модулю.* Изъ двухъ сравненій

$$a \equiv c \text{ (mod. } k), \qquad b \equiv c \text{ (mod. } k)$$

вытекаетъ третье

$$a \equiv b \text{ (mod. } k).$$

$a-c=k.t$
$b-c=k.s$
$a-b=k(t-s)$

3°. *Прибавляя къ обѣимъ частямъ сравненія по одному и тому же числу, сравненіе не нарушаемъ.*

Изъ сравненія

$$a \equiv b \pmod{k}$$

выводимъ

$$a + c \equiv b + c \pmod{k}$$

или

$$a - c \equiv b - c \pmod{k}.$$

$a - b = k.t$
$(a-c)-(b-c) = k.t$

4°. *Во всякомъ сравненіи, совершенно такъ, какъ и во всякомъ уравненіи, члены могутъ быть переносимы изъ одной части въ другую.* Напримѣръ, изъ сравненія

$$a + b \equiv c + d \pmod{k}$$

выводимъ

$$a - c \equiv d - b \pmod{k}.$$

$(a+b)-(c+d) = k.t$
$(a-c)-(d-b) = k.t$

5°. *Два или нѣсколько сравненій съ однимъ и тѣмъ же модулемъ могутъ быть почленно складываемы или вычитаемы.* Такъ, изъ двухъ сравненій

$$a \equiv b \pmod{k}, \qquad a' \equiv b' \pmod{k}$$

выводимъ

$$a \pm a' \equiv b \pm b' \pmod{k},$$

$a - b = k.t$
$a' - b' = k.t'$
$(a \pm a') - (b \pm b') = k$

гдѣ можно брать или верхніе знаки, или нижніе.

6. *Сравненіе не нарушается, если обѣ его части умножить на одно и то же цѣлое число.* Изъ сравненія

$$a \equiv b \pmod{k}$$

вытекаетъ

$$ac \equiv bc \pmod{k}.$$

$a - b = k.t$
$ac - bc = k.tc$

7°. *Два или нѣсколько сравненій съ однимъ и тѣмъ же модулемъ могутъ быть почленно перемножаемы.*

Предложеніе это, хотя и не столь очевидно, какъ предшествующія, провѣряется непосредственно. На самомъ дѣлѣ, два сравненія

$$a \equiv b \ (\text{mod.}\ k), \qquad a' \equiv b' \ (\text{mod.}\ k)$$

показываютъ, что числа

$$\frac{a-b}{k} = t, \qquad \frac{a'-b'}{k} = t'$$

суть цѣлыя. Изъ выраженій этихъ чиселъ получаемъ уравненія

$$a = b + kt, \qquad a' = b' + kt',$$

которыя перемножая почленно, находимъ

$$aa' = bb' + k\,(bt' + b't + ktt').$$

Результатъ этотъ показываетъ, что разность $aa' - bb'$ дѣлится на k, то есть

$$aa' \equiv bb' \ (\text{mod.}\ k).$$

8°. *Сравненіе не нарушается, если обѣ его части возвысимъ въ одну и ту же степень.*

Само собою разумѣется, что тутъ идетъ рѣчь о цѣлой положительной степени. Предложеніе это есть слѣдствіе предыдущаго.

9°. *Если $f(x)$ изображаетъ цѣлую функцію съ цѣлыми коэффиціентами, и если два числа a и b сравнимы между собою по модулю k, то значенія $f(a)$ и $f(b)$ также сравнимы между собою по тому же модулю k.*

Дѣйствительно, изъ сравненія

$$a \equiv b \ (\text{mod.}\ k),$$

какъ слѣдствіе, вытекаетъ рядъ такихъ сравненій:

$$Aa^n \equiv Ab^n \pmod{k},$$

$$A_1a^{n-1} \equiv A_1b^{n-1} \pmod{k},$$

$$A_2a^{n-2} \equiv A_2b^{n-2} \pmod{k},$$

. . . .

. . . .

$$A_{n-1}a \equiv A_{n-1}b \pmod{k},$$

$$A_n \equiv A_n \pmod{k},$$

гдѣ n есть произвольное цѣлое положительное число; $A, A_1, A_2, \ldots$ произвольныя цѣлыя числа; впрочемъ, послѣднее сравненіе очевидно само по себѣ. Складывая всѣ эти сравненія и полагая для сокращенія

$$Ax^n + A_1x^{n-1} + \ldots + A_n = f(x),$$

получаемъ

$$f(a) \equiv f(b) \pmod{k}.$$

10°. *Если двѣ цѣлыя функціи съ цѣлыми коэффиціентами $f(x)$ и $f_1(x)$ таковы, что коэффиціенты у подобныхъ членовъ въ ихъ выраженіяхъ сравнимы между собою по модулю k, и если числа a и b также сравнимы между собою по модулю k, то тогда значенія $f(a)$ и $f_1(b)$ сравнимы между собою по тому же модулю k.*

Дѣйствительно, изъ сравненія

$$a \equiv b \pmod{k}$$

какъ слѣдствіе, вытекаютъ слѣдующія:

$$a^n \equiv b^n \pmod{k},$$

$$a^{n-1} \equiv b^{n-1} \pmod{k},$$

. . . .

. . . .

$$a \equiv b \pmod{k},$$

$$1 \equiv 1 \pmod{k}.$$

Перемножая эти сравненія соотвѣтственно на сравненія

$$A \equiv B \pmod{k},$$
$$A_1 \equiv B_1 \pmod{k},$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$A_{n-1} \equiv B_{n-1} \pmod{k},$$
$$A_n \equiv B_n \pmod{k},$$

причемъ нѣкоторые изъ чиселъ A могутъ быть равны 0; это же относится и къ числамъ B.

получаемъ

$$Aa^n \equiv Bb^n \pmod{k},$$
$$A_1a^{n-1} \equiv B_1b^{n-1} \pmod{k},$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$A_{n-1}a \equiv B_{n-1}b \pmod{k},$$
$$A_n \equiv B_n \pmod{k}.$$

Складывая эти послѣднія, находимъ

$$f(a) \equiv f_1(b) \pmod{k},$$

что и слѣдовало доказать.

Слѣдуетъ здѣсь замѣтить, что предложеніе n^0 9 составляетъ частный случай n^0 10.

11°. *Сравненіе не нарушается если обѣ его части а также и модуль умножить или раздѣлить на одно и то же число.* Изъ сравненія

$$a \equiv b \pmod{k}$$

$a - b = k.t$

вытекаетъ

$ac - bc = (kc).t$ (см. n°6).

$$ac \equiv bc \pmod{kc};$$

и обратно, изъ послѣдняго вытекаетъ предшествующее.

12°. *Если* $a \equiv b$ (mod. k), *то общій наибольшій дѣлитель чиселъ a и k совпадаетъ съ общимъ наибольшимъ дѣлителемъ чиселъ b и k.* Ибо тогда имѣемъ уравненіе

$$a = b + kt,$$

которое показываетъ, что всякій общій дѣлитель чиселъ a и k будетъ общимъ дѣлителемъ чиселъ b и k, равно какъ и обратно: всякій общій дѣлитель чиселъ b и k будетъ общимъ дѣлителемъ чиселъ a и k. Но дѣлитель a и b можетъ и не быть дѣлителемъ k; напр. $42 \equiv 7$ ...

13°. *Если* $a \equiv b$ (mod. k), *и b есть число простое относительно k, то a есть также число простое относительно k.*

Предложеніе это есть слѣдствіе предшествующаго.

14°. *Если* $ab \equiv 0$ (mod. k), *и если множитель a есть простой относительно k, то тогда* $b \equiv 0$ (mod. k).

На самомъ дѣлѣ, произведеніе ab, по предположенію, дѣлится на k и, кромѣ того, числа a и k относительно простыя; поэтому, на основаніи теоремы 2-ой, n^0 4, стр. 6 заключаемъ, что b дѣлится на k, то есть $b \equiv 0$ (mod. k).

15°. *Члены сравненія могутъ быть сокращены на ихъ общій множитель, если этотъ множитель число простое съ модулемъ.*

На самомъ дѣлѣ, изъ сравненія

$$ma \equiv mb \text{ (mod. } k)$$

выводимъ

$$m(a - b) \equiv 0 \text{ (mod. } k),$$

а такъ какъ m число простое съ k, то, на основаніи вышедоказаннаго, заключаемъ

$$a - b \equiv 0 \text{ (mod. } k),$$

или

$$a \equiv b \text{ (mod. } k).$$

$ma - mb = k.t$
$m(a-b) = k.t$
$a - b = k.\frac{t}{m}$

16°. *Если число a простое относительно k, то два сравненія вида*

$$aa' \equiv bb' \text{ (mod. } k),$$

$$a \equiv b \text{ (mod. } k)$$

можно раздѣлить почленно первое на второе и написать

$$a' \equiv b' \text{ (mod. } k).$$

Дѣйствительно, изъ сравненія $a \equiv b$ (mod. k) выводимъ

$$ab' \equiv bb' \text{ (mod. } k).$$

Сличая это сравненіе со сравненіемъ $aa' \equiv bb'$ (mod. k), находимъ

$$aa' \equiv ab' \text{ (mod. } k).$$

Отсюда, сокращая обѣ части на a, получаемъ

$$a' \equiv b' \text{ (mod. } k).$$

17°. *Два числа, сравнимыя между собою по двумъ или нѣсколькимъ модулямъ, сравнимы и по наименьшему кратному этихъ модулей.* Ибо разность $a - b$, дѣлясь на каждое изъ чиселъ k, k', k'', . . ., дѣлится и на наименьшее кратное этихъ послѣднихъ.

18°. *Сравненіе не нарушается, если модуль замѣнить какимъ либо изъ его дѣлителей.*

§ II. О наименьшихъ вычетахъ. Распредѣленіе чиселъ на классы по данному модулю.

Опредѣленіе наименьшихъ вычетовъ.

26. Всѣ числа, сравнимыя съ a по модулю k, или, другими словами, всѣ рѣшенія сравненія

$$x \equiv a \text{ (mod. } k)$$ или $a \equiv x$ (mod. k)

выражаются общею формулой

$$x = a - kt,$$

гдѣ t означаетъ цѣлое число, принимающее всевозможныя значенія. Число $a - kt$ называется вычетомъ числа a.

Чтобы узнать сколько въ ряду

(1) . . . . 0, 1, 2, 3, . . . $k-1$

находится чиселъ сравнимыхъ съ a по модулю k, составляемъ условія

$$0 \leqq a - kt < k,$$

откуда выводимъ

$$-a \leqq -kt < -a+k$$
$$a-k < kt \leqq a$$

$$\frac{a}{k} - 1 < t \leqq \frac{a}{k}.$$

Неравенства эти показываютъ, что существуетъ одно и только одно частное значеніе для t, при которомъ число $a - kt$ будетъ содержаться въ (1). Это число называютъ *наименьшимъ положительнымъ вычетомъ* числа a; названіе, какъ видимъ, отвѣчаетъ характеристическому свойству числа.

Наименьшій положительный вычетъ можетъ равняться нулю; это имѣетъ мѣсто въ томъ только случаѣ, если число дѣлится на модуль.

Подобно предыдущему легко удостовѣриться, что въ ряду

$$0, -1, -2, -3, \ldots -(k-1),$$

находится одно и только одно число, сравнимое съ a по модулю k. Искомое число должно быть вида $a - kt$ и должно удовлетворять условіямъ

$$-k < a - kt \leqq 0,$$

откуда выводимъ

$$-k-a < -kt \leqq -a$$
$$a \leqq kt < k+a$$

$$\frac{a}{k} \leqq t < 1 + \frac{a}{k}.$$

Неравенства эти опредѣляютъ вполнѣ число t, равно какъ и соотвѣтствующее ему число $a - kt$. Это послѣднее называется *наименьшимъ отрицательнымъ вычетомъ* числа a; оно равно нулю въ томъ только случаѣ, когда a дѣлится на k.

27. Изображая чрезъ r наименьшій положительный вычетъ числа a по модулю k, а чрезъ $-s$ наименьшій отрицательный вычетъ того же числа a по модулю k, имѣемъ два случая:

1°. *Если a дѣлится на k, то* $t = \frac{a}{k}$ и $r = s = a - kt = 0$

$$r = -s = 0.$$

2°. *Если a не дѣлится на k, то*

$$r + s = k.$$

Первый случай былъ отмѣченъ ранѣе; что касается втораго, то тогда имѣемъ неравенства

$$0 < r < k,$$

откуда выводимъ

$$-k < r - k < 0,$$

а это показываетъ, что

$$r - k = -s.$$

На основаніи этого равенства мы заключаемъ, что одинъ изъ двухъ наименьшихъ вычетовъ по числовой величинѣ не превышаетъ половины модуля. Если числовая величина одного изъ наименьшихъ вычетовъ равна $\frac{k}{2}$, то числовая величина остальнаго также равна $\frac{k}{2}$; разумѣется, что это можетъ имѣть мѣсто только при четномъ модулѣ. Изъ всего видно, что числовыя величины наименьшихъ вычетовъ только въ двухъ случаяхъ бываютъ равными другъ другу: во первыхъ, если число дѣлится на модуль; тогда $r = s = 0$, и, во вторыхъ, если модуль четный и число дѣлится на половину модуля; тогда $r = s = \frac{k}{2}$. Внѣ этихъ двухъ случаевъ всегда одинъ изъ наименьшихъ вычетовъ по числовой величинѣ $> \frac{k}{2}$, другой $< \frac{k}{2}$. Этотъ послѣдній называется *абсолютно малымъ вычетомъ*.

Примѣръ 1. Опредѣлить наименьшіе вычеты 127 по модулю 17.

Раздѣляя 127 на 17 находимъ частное 7, остатокъ 8; слѣдовательно имѣемъ

$$127 \equiv 8 \text{ (mod. 17)}$$

и очевидно, что $r = 8$.

Наименьшій отрицательный вычетъ опредѣляется по формулѣ

$$-s = r - k = 8 - 17 = -9.$$

Абсолютно малый вычетъ равенъ 8.

Примѣръ 2. Опредѣлить наименьшіе вычеты числа — 200 по модулю 13.

Раздѣляя 200 на 13 находимъ частное 15, остатокъ 5; слѣдовательно

$$200 \equiv 5 \pmod{13}.$$

Отсюда выводимъ

$$-200 \equiv -5 \pmod{13},$$

и заключаемъ, что — 5 есть наименьшій отрицательный вычетъ.

Наименьшій положительный вычетъ равенъ

$$-5 + 13 = 8.$$

Абсолютно малый вычетъ есть — 5.

28. Провѣримъ здѣсь справедливость одного предложенія, относящагося къ знаку абсолютно малаго вычета; оно понадобится намъ впослѣдствіи. При этомъ, понятно, будемъ предполагать, что число не дѣлится ни на модуль, ни на половину модуля и, что оно положительно. Доказательство одного предложенія.

Предложеніе состоитъ въ слѣдующемъ.

Если e изображаетъ единицу, взятую со знакомъ абсолютно малаго вычета числа a по модулю k, то

$$e = (-1)^{E\frac{2a}{k}}.$$

Въ самомъ дѣлѣ, обозначая чрезъ q и r частное и остатокъ отъ дѣленія a на k, имѣемъ равенство

$$a = qk + r,$$

откуда выводимъ

$$\frac{2a}{k} = 2q + \frac{2r}{k}.$$

Если $r < \frac{k}{2}$, то r есть абсолютно малый вычетъ числа a и слѣдовательно $e = 1$. Съ другой стороны, послѣднее равенство показываетъ, что цѣлая часть дроби $\frac{2a}{k}$ равна $2q$, вслѣдствіе чего имѣемъ

$$(-1)^{E\frac{2a}{k}} = (-1)^{2q} = 1 = e,$$

а это согласно съ предложеніемъ.

Если же $r > \frac{k}{2}$, то абсолютно малый вычетъ числа a равенъ $r - k$, и поэтому $e = -1$. Тогда, написавъ предыдущее равенство такъ:

$$\frac{2a}{k} = 2q + 1 + \frac{2r - k}{k},$$

мы замѣчаемъ, что послѣдній членъ во второй части представляетъ правильную положительную дробь; вслѣдствіе чего заключаемъ, что цѣлая часть дроби $\frac{2a}{k}$ равна $2q + 1$. Слѣдовательно

$$(-1)^{E\frac{2a}{k}} = (-1)^{2q+1} = -1 = e.$$

Это согласно съ предложеніемъ, которое такимъ образомъ вполнѣ доказано.

Распредѣленіе чиселъ на классы.

29. Изъ того, что всякое число сравнимо по модулю k съ однимъ только числомъ въ ряду $0, 1, 2, \ldots k - 1$, вытекаетъ возможность распредѣлить всѣ числа на классы такъ, чтобы всякое число принадлежало къ одному только классу. Въ самомъ дѣлѣ, если согласимся зачислять къ одному классу всѣ числа, имѣющія одинъ и тотъ же наименьшій положительный вычетъ, то тогда всѣ числа, какъ положительныя такъ и отрицательныя, распредѣлятся между k-различными классами. Каждое изъ чиселъ, принадлежащихъ къ какому либо классу, опредѣляетъ собою всѣ остальныя числа того же класса, то есть опредѣляетъ собой самый классъ и потому можетъ служить его представителемъ. Ибо числа, принадлежащія къ одному классу, всѣ сравнимы между собой, равно и наоборотъ: два числа, сравнимыя между собою принадлежатъ къ одному классу.

Взявъ отъ каждаго класса по одному какому нибудь числу, получаемъ *полную систему несравнимыхъ чиселъ, или полную систему представителей классовъ*

$$a_1,\ a_2,\ a_3,\ldots a_k,$$

характеристическое свойство которой состоитъ въ томъ, что каждыя два числа, входящія въ ея составъ, несравнимы между собой по модулю k. Этотъ признакъ можно выразить въ другой формѣ такъ: всякое произвольно взятое число сравнимо по модулю k съ однимъ, и только съ однимъ изъ чиселъ означенной полной системы.

Простѣйшими полными системами несравнимыхъ чиселъ можно считать двѣ слѣдующія:

$$0,\ 1,\ 2,\ldots k-1$$

и

$$0,\ -1,\ -2,\ldots -(k-1).$$

Вообще, k цѣлыхъ чиселъ, идущія въ натуральномъ порядкѣ, начиная съ произвольнаго a,

$$a,\ a+1,\ a+2,\ldots a+k-1,$$

очевидно составляютъ полную систему несравнимыхъ чиселъ.

Каждое изъ чиселъ полной системы можно увеличивать или уменьшать на произвольную кратность модуля; система не перестаетъ оставаться послѣ этого полной.

§ III. Теорема Фермата.

30. Начала, изложенныя въ предыдущихъ параграфахъ, даютъ возможность доказать одну изъ важнѣйшихъ теоремъ въ теоріи чиселъ, высказанную въ первый разъ Ферматомъ. Мы считаемъ не лишнимъ привести здѣсь два различныхъ ея доказательства; впослѣдствіи будемъ имѣть случай сообщить еще третье, независимое отъ предыдущихъ. Первое доказательство.

Чтобъ не повторяться, начнемъ прямо съ доказательства теоремы болѣе общей чѣмъ теорема Фермата, которую потому и называютъ *обобщенной теоремой Фермата;* она принадлежитъ Эйлеру.

Теорема 1. *Если a число простое относительно k, то*

$$a^{\varphi(k)} \equiv 1 \pmod{k},$$

гдѣ $\varphi(k)$ изображаетъ число чиселъ простыхъ съ k и $< k$.

Обозначивъ чрезъ $a_1, a_2, \ldots a_m$ всѣ числа простыя съ k и $< k$, такъ что $m = \varphi(k)$, составляемъ произведенія

$$aa_1, aa_2, aa_3, \ldots aa_m$$

и соотвѣтствующіе имъ наименьшіе положительные вычеты

$$b_1, b_2, b_3, \ldots b_m.$$

Имѣемъ рядъ сравненій

$$\left.\begin{array}{r} aa_1 \equiv b_1, \\ aa_2 \equiv b_2, \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ aa_m \equiv b_m, \end{array}\right\} \pmod{k},$$

которыя перемножая почленно, получаемъ

$$(1) \ldots\ldots a^m a_1 a_2 \ldots a_m \equiv b_1 b_2 \ldots b_m \pmod{k}.$$

Всѣ числа въ ряду $b_1, b_2, \ldots b_m$ различны; ибо, допустивъ $b_i = b_j$, мы имѣли бы сравненіе

$$aa_i \equiv aa_j \pmod{k},$$

которое по сокращеніи на a даетъ

$$a_i \equiv a_j \pmod{k},$$

что невозможно.

Сверхъ того очевидно, что каждое изъ чиселъ $b_1, b_2, \ldots$ содержится въ ряду чиселъ $a_1, a_2, \ldots$; ибо произведенія aa_1, $aa_2, \ldots$, будучи простыми относительно k, ихъ вычеты суть также простые относительно k.

Слѣдовательно рядъ чиселъ $b_1, b_2, \ldots$ составляетъ нѣкоторую перестановку чиселъ $a_1, a_2, \ldots$, на основаніи чего заключаемъ

$$a_1 a_2 \ldots a_m = b_1 b_2 \ldots b_m.$$

Равенство это показываетъ, что обѣ части сравненія (1) имѣютъ общій множитель, который очевидно простой относительно k. Сокращая на этотъ множитель, получаемъ

$$a^m \equiv 1 \ (\mathrm{mod.}\ k),$$

или, замѣчая что $m = \varphi(k)$,

$$a^{\varphi(k)} \equiv 1 \ (\mathrm{mod.}\ k),$$

что и слѣдовало доказать.

Представляя модуль въ видѣ произведенія изъ простыхъ множителей, послѣднюю теорему можемъ выразить такъ:

$$a^{p_1^{\alpha_1-1} p_2^{\alpha_2-1} \ldots (p_1-1)(p_2-1)\ldots} \equiv 1 \ (\mathrm{mod.}\ p_1^{\alpha_1} p_2^{\alpha_2} \ldots).$$

Теорема Фермата относится къ случаю, когда модуль простой; она состоитъ въ слѣдующемъ.

Теорема 2. *Если a не дѣлится на простое число p, то*

$$a^{p-1} \equiv 1 \ (\mathrm{mod.}\ p).$$

Слѣдствіе. *Каково бы ни было число a, если число p простое, то*

$$a^p \equiv a \ (\mathrm{mod.}\ p).$$

Это сравненіе очевидно въ томъ случаѣ, когда a дѣлится на p; если же a не дѣлится на p, оно выводится изъ предшествующаго сравненія, умноженіемъ обѣихъ частей на a.

Слѣдуетъ однако замѣтить здѣсь, что по содержанію слѣдствіе вполнѣ равносильно теоремѣ; ибо обѣ части послѣдняго сравненія можно сократить на a, если только a не дѣлится на p, и получается тогда теорема Фермата.

31. *Второе доказательство теоремы Фермата.* Многія формулы, алгебраическія или даже трансцендентныя, даютъ возможность выводить различныя свойства цѣлыхъ чиселъ. Простѣйшій примѣръ въ этомъ родѣ представляетъ биномъ Ньютона

$$(a+b)^p = a^p + \frac{p}{1} a^{p-1} b + \frac{p(p-1)}{1.2} a^{p-2} b^2 + \ldots + b^p,$$

изъ котораго весьма легко вывести теорему Фермата.

Дѣйствительно, предположивъ, что p число простое, мы замѣчаемъ, что всѣ коэффиціенты во второй части, за исключеніемъ двухъ крайнихъ, дѣлятся на p; поэтому можемъ написать

$$(1) \ldots\ldots\ldots \quad (a+b)^p \equiv a^p + b^p \pmod{p},$$

и сравненіе это имѣетъ мѣсто при всякихъ цѣлыхъ числахъ a и b.

Внося въ обѣихъ частяхъ $b+c$ на мѣсто b, получаемъ

$$(a+b+c)^p \equiv a^p + (b+c)^p \pmod{p};$$

съ другой стороны имѣемъ

$$(b+c)^p \equiv b^p + c^p \pmod{p};$$

слѣдовательно

$$(a+b+c)^p \equiv a^p + b^p + c^p \pmod{p}.$$

Вообще, изъ (1) выводимъ

$$(a+b+\ldots+l)^p \equiv a^p + b^p + \ldots + l^p \pmod{p},$$

гдѣ число чиселъ $a, b, \ldots l$ совершенно произвольно. Отсюда, полагая сперва $a = b = \ldots = l = 1$, и полагая затѣмъ, что число такихъ единицъ равно произвольному числу a, находимъ

$$a^p \equiv a \pmod{p}.$$

Предполагая, что a не дѣлится на p и сокращая обѣ части на a, получаемъ теорему Фермата 3е доказательство см. п. стр.

$$a^{p-1} \equiv 1 \ (\text{mod.}\ p).$$

32. Изъ теоремы Фермата легко вывести обобщенную теорему, которая въ началѣ параграфа была доказана независимо; для этого стоитъ только принять во вниманіе слѣдующую лемму. Теорема Эйлера.

Лемма. *Если имѣетъ мѣсто сравненіе*

$$a \equiv b \ (\text{mod.}\ p^n),$$

то имѣетъ мѣсто и сравненіе

$$a^{p^m} \equiv b^{p^m} \ (\text{mod.}\ p^{n+m}),$$

гдѣ m произвольное цѣлое положительное число; число p предполагается простымъ.

Дѣйствительно, изъ сравненія, которое предполагается въ леммѣ, вытекаетъ уравненіе

$$a = b + tp^n,$$

обѣ части котораго возвышая въ p-ую степень, получаемъ

$$a^p = b^p + \frac{p}{1} b^{p-1} tp^n + \frac{p(p-1)}{1.2} b^{p-2} t^2 p^{2n} + \ldots$$

Каждый членъ во второй части, кромѣ перваго, дѣлится на p^{n+1}; поэтому имѣемъ сравненіе

$$a^p \equiv b^p \ (\text{mod.}\ p^{n+1}).$$

Принимая его за начальное и повторяя прежній пріемъ, получаемъ

$$a^{p^2} \equiv b^{p^2} \ (\text{mod.}\ p^{n+2}).$$

Продолжая дѣйствовать подобнымъ образомъ далѣе, получаемъ рядъ сравненій вида

$$a^{p^m} \equiv b^{p^m} \ (\text{mod.}\ p^{n+m}),$$

гдѣ $m = 1, 2, 3, \ldots \infty$.

Удостовѣрившись въ справедливости леммы, переходимъ къ выводу обобщенной теоремы Фермата.

Если a число простое съ k, а это послѣднее, будучи разложено на простые множители, представляется въ видѣ $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$, то, основываясь на теоремѣ Фермата, мы можемъ написать такой рядъ сравненій:

$$a^{p_1-1} \equiv 1 \pmod{p_1},$$
$$a^{p_2-1} \equiv 1 \pmod{p_2},$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$a^{p_m-1} \equiv 1 \pmod{p_m}.$$

Примѣняя къ каждому изъ нихъ предыдущую лемму, выводимъ

$$a^{p_1^{\alpha_1-1}(p_1-1)} \equiv 1 \pmod{p_1^{\alpha_1}},$$
$$a^{p_2^{\alpha_2-1}(p_2-1)} \equiv 1 \pmod{p_2^{\alpha_2}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a^{p_m^{\alpha_m-1}(p_m-1)} \equiv 1 \pmod{p_m^{\alpha_m}}.$$

Возвышеніемъ обѣихъ частей каждаго изъ этихъ сравненій въ соотвѣтствующія степени получаемъ

$$a^{\varphi(k)} \equiv 1 \pmod{p_1^{\alpha_1}},$$
$$a^{\varphi(k)} \equiv 1 \pmod{p_2^{\alpha_2}},$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$a^{\varphi(k)} \equiv 1 \pmod{p_m^{\alpha_m}}.$$

Отсюда заключаемъ

$$a^{\varphi(k)} \equiv 1 \pmod{k};$$

что и слѣдовало доказать.

Примѣръ 1. Повѣрить теорему Фермата въ случаѣ $p = 13$, $a = 10$.

Такъ какъ $10 \equiv -3 \pmod{13}$, то слѣдовательно $10^{12} \equiv (-3)^{12} \equiv 3^{12} \pmod{13}$. Далѣе, находимъ $3^2 \equiv -4 \pmod{13}$; слѣдовательно $3^{12} \equiv (-4)^6 \equiv 4^6 \pmod{13}$. Продолжая далѣе, находимъ $4^2 \equiv 3 \pmod{13}$; слѣдовательно $4^6 \equiv 3^3 \equiv 27 \equiv 1 \pmod{13}$. Сличая между собою полученныя сравненія, заключаемъ $10^{12} \equiv 1 \pmod{13}$.

Примѣръ 2. Повѣрить теорему Эйлера въ случаѣ $k = 100$, $a = 63$.

Имѣемъ $\varphi(100) = \varphi(4)\varphi(25) = 40$. Такъ какъ $63^2 = 3969$, то $63^2 \equiv -31$, и $63^{40} \equiv 31^{20} \pmod{100}$. Возвышая 31 въ квадратъ, находимъ $31^2 = 961$; слѣдовательно $31^2 \equiv -39 \pmod{100}$; отсюда $31^{20} \equiv 39^{10}$. Вычисляя далѣе, находимъ $39^2 = 1521$; слѣдовательно $39^2 \equiv 21 \pmod{100}$; отсюда $39^{10} \equiv 21^5$. Далѣе, находимъ $21^2 = 441$; слѣдовательно $21^2 \equiv 41 \pmod{100}$; отсюда $21^4 \equiv 41^2$. Возвышая 41 въ квадратъ, получаемъ 1681; слѣдовательно $41^2 \equiv 81 \pmod{100}$. Сличая предыдущія сравненія, находимъ $63^{40} \equiv 21.81 \pmod{100}$; но $21.81 = 1701$; слѣдовательно $63^{40} \equiv 1 \pmod{100}$.

§ IV. Слѣдствія изъ теоремы Фермата.

33. **Теорема.** *Если p число простое и нечетное, а a не дѣлится на p, то степень $a^{\frac{p-1}{2}}$ сравнима по модулю p съ однимъ изъ чиселъ ± 1.*

Дѣйствительно, сравненіе

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

можно написать такъ:

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p},$$

а это тогда только возможно, когда имѣетъ мѣсто одно изъ двухъ сравненій

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (mod. } p),$$

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (mod. } p).$$

Одновременно оба эти сравненія не могутъ имѣть мѣста потому, что тогда мы имѣли бы $1 \equiv -1$ (mod. p), или $2 \equiv 0$ (mod. p); между тѣмъ по предположенію 2 не дѣлится на p.

По примѣру Лежандра принято обозначать символомъ $\left(\frac{a}{p}\right)$ то изъ чиселъ $+1$, -1, которое сравнимо по модулю p со степенью $a^{\frac{p-1}{2}}$. Значеніе этого символа представляетъ функцію чиселъ a и p, причемъ p должно быть простымъ и не равнымъ 2, а a не должно дѣлиться на p.

Вычисленіе символа Лежандра приводится всегда къ опредѣленію знака, ибо числовая его величина равна 1.

Въ послѣдующихъ главахъ увидимъ, какую роль въ теоріи чиселъ играетъ означенный символъ, и какими обладаетъ онъ свойствами.

Если число p не велико, значеніе $\left(\frac{a}{p}\right)$ можетъ быть опредѣлено непосредственно безъ особыхъ затрудненій.

Примѣръ 1. Опредѣлить значенія $\left(\frac{a}{3}\right)$ для $a = 1, 2$.

Находимъ

$$1^{\frac{3-1}{2}} = 1, \quad 2^{\frac{3-1}{2}} = 2 \equiv -1 \text{ (mod. 3)};$$

слѣдовательно

$$\left(\frac{1}{3}\right) = 1, \quad \left(\frac{2}{3}\right) = -1.$$

Примѣръ 2. Опредѣлить значенія $\left(\frac{a}{5}\right)$ для $a = 1, 2, 3, 4$.

Находимъ

$$1^2 = 1; \quad 2^2 = 4 \equiv -1 \text{ (mod. 5)}; \quad 3^2 \equiv -1 \text{ (mod. 5)};$$

$$4^2 \equiv 1 \text{ (mod. 5)};$$

слѣдовательно

$$\left(\frac{1}{5}\right)=1,\ \left(\frac{2}{5}\right)=-1,\ \left(\frac{3}{5}\right)=-1,\ \left(\frac{4}{5}\right)=1.$$

Примѣръ 3. Опредѣлить значенія $\left(\frac{a}{7}\right)$ для $a=1, 2, 3, 4, 5, 6$.

Находимъ

$$1^3\equiv 1,\quad 2^3\equiv 1,\quad 3^3\equiv -1,\quad 4^3\equiv 1,\quad 5^3\equiv -1,\quad 6^3\equiv -1 \pmod{7};$$

слѣдовательно

$$\left(\frac{1}{7}\right)=1,\ \left(\frac{2}{7}\right)=1,\ \left(\frac{3}{7}\right)=-1,\ \left(\frac{4}{7}\right)=1,\ \left(\frac{5}{7}\right)=-1,$$
$$\left(\frac{6}{7}\right)=-1.$$

34. Выведемъ еще нѣсколько предложеній, легко получаемыхъ изъ теоремы Фермата. Впослѣдствіи они будутъ вновь получены, помощью болѣе спеціальныхъ пріемовъ, въ связи съ другими вопросами; тѣмъ не менѣе мы желаемъ остановиться на нихъ здѣсь, чтобъ взглянуть на предметъ съ точки зрѣнія болѣе обычной, по преимуществу алгебраической, пользуясь формулой бинома Ньютона, какъ вспомогательнымъ средствомъ. Теорема Вильсона.

Теорема 1. *Если p число простое, а m дѣлится на $p-1$, то*

$$S_m = 1^m + 2^m + 3^m + \ldots + (p-1)^m \equiv -1 \pmod{p};$$

если же m не дѣлится на $p-1$, то

$$S_m = 1^m + 2^m + 3^m + \ldots + (p-1)^m \equiv 0 \pmod{p}.$$

p-1 всегда число четное. Если m нечетное, то оно не дѣлится на p-1, и эта часть теоремы отпадаетъ, и может быть осуществлена только вторая часть. Если m нечетное, то a^m+b^m дѣлится на $a+b$, т. е. $i^m+(p-i)^m$ дѣлится на $i+p-i=p$.

1. При нечетномъ m теорема очевидна, ибо тогда сумма членовъ равно удаленныхъ отъ концовъ въ первой части сравненія дѣлится на p.

2. Переходя къ доказательству теоремы при четномъ m, мы положимъ сначала, что m дѣлится на $p-1$,

$$m=(p-1)t.$$

Если m [illegible], то может быть осуществлена одна изъ двухъ [illegible] теоремы.

По теоремѣ Фермата имѣемъ рядъ сравненій

$$1^{p-1} \equiv 1 \ (\text{mod.}\, p),$$

$$2^{p-1} \equiv 1 \ (\text{mod.}\, p),$$

. . . .

. . . .

$$(p-1)^{p-1} \equiv 1 \ (\text{mod.}\, p).$$

Возвышая обѣ части каждаго изъ этихъ сравненій въ степень m, получаемъ

$$1^m \equiv 1 \ (\text{mod.}\, p),$$

$$2^m \equiv 1 \ (\text{mod.}\, p),$$

. . . .

. . . .

$$(p-1)^m \equiv 1 \ (\text{mod.}\, p);$$

отсюда, складывая почленно, находимъ

$$1^m + 2^m + \ldots + (p-1)^m \equiv p-1 \ (\text{mod.}\, p)$$

или, проще,

$$1^m + 2^m + \ldots + (p-1)^m \equiv -1 \ (\text{mod.}\, p).$$

3. Остается доказать справедливость теоремы во второмъ случаѣ, когда m не дѣлится на $p-1$.

Положивъ для сокращенія

$$S_m = 1^m + 2^m + 3^m + \ldots + (p-1)^m,$$

мы замѣчаемъ, что при доказательствѣ можно ограничиться предположеніемъ $m < p-1$; ибо въ противномъ случаѣ, полагая

$$m = (p-1)t + m',$$

гдѣ m' есть остатокъ отъ дѣленія m на $p-1$ и потому $0 < m' < p-1$, имѣемъ

$$1^m \equiv 1^{m'},\ 2^m \equiv 2^{m'}, \ldots (p-1)^m \equiv (p-1)^{m'}\ (\text{mod.}\, p),$$

откуда, складывая, получаемъ

$$S_m \equiv S_{m'}\ (\text{mod.}\, p).$$

и если окажется, что $S_{m'} \equiv -1$ (mod. p), то необходимо будетъ $S_m \equiv -1$ (mod. p)

Принимая это во вниманіе, переходимъ къ тожественному уравненію

$$(x+1)^m - x^m = \frac{m}{1}x^{m-1} + \frac{m(m-1)}{1.2}x^{m-2} + \ldots + 1,$$

и приравниваемъ послѣдовательно $x = 1, 2, \ldots p-1$; получаемъ

$$2^m - 1 = \frac{m}{1} + \frac{m(m-1)}{1.2} + \ldots + 1,$$

$$3^m - 2^m = \frac{m}{1}2^{m-1} + \frac{m(m-1)}{1.2}2^{m-2} + \ldots + 1,$$

. . . .

. . . .

$$p^m - (p-1)^m = \frac{m}{1}(p-1)^{m-1} + \frac{m(m-1)}{1.2}(p-1)^{m-2} + \ldots + 1,$$

Отсюда, складывая почленно, находимъ

$$p^m - 1 = \frac{m}{1}S_{m-1} + \frac{m(m-1)}{1.2}S_{m-2} + \ldots + S_0,$$

или, перенося S_0 въ первую часть,

$$p(p^{m-1} - 1) = \frac{m}{1}S_{m-1} + \frac{m(m-1)}{1.2}S_{m-2} + \ldots + \frac{m}{1}S_1.$$

Дѣлая въ этой формулѣ послѣдовательно $m = 2, 3, 4, \ldots p-1$, получаемъ рядъ сравненій:

$$\left.\begin{array}{l} 2S_1 \equiv 0, \\ 3S_2 + 3S_1 \equiv 0, \\ 4S_3 + 6S_2 + 4S_1 \equiv 0, \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ (p-1)S_{p-2} + \frac{(p-1)(p-2)}{1.2}S_{p-3} + \ldots + (p-1)S_1 \equiv 0 \end{array}\right\} (\text{mod.}\, p),$$

Для S_{p-1} доказ. не требуется, ибо въ этомъ случаѣ $m=p-1$ дѣлится на $p-1$.

изъ которыхъ поочередно выводимъ

$$S_1 \equiv 0, \quad S_2 \equiv 0, \quad S_3 \equiv 0, \ldots S_{p-2} \equiv 0 \pmod{p}.$$

Такъ теорема наша доказана вполнѣ.

Теорема 2. *Изображая соотвѣтственно чрезъ $q_1, q_2, \ldots q_{p-1}$ сумму всевозможныхъ произведенiй изъ чиселъ $1, 2, \ldots p-1$ по одному, по два, по три и т. д., имѣемъ рядъ такихъ сравненiй:*

$$q_1 \equiv q_2 \equiv \ldots \equiv q_{p-2} \equiv 0, \quad q_{p-1} \equiv -1 \pmod{p}.$$

Доказательство. Разсматривая x какъ перемѣнную, имѣемъ тожество

$$(x-1)(x-2)\ldots(x-p+1) = x^{p-1} - q_1 x^{p-2} + q_2 x^{p-3} - \ldots \pm q_{p-1},$$

въ которомъ полагаемъ послѣдовательно $x = 1, 2, 3, \ldots p-1$; получаемъ

$$1 - q_1 + q_2 - q_3 + \ldots \pm q_{p-1} = 0,$$
$$2^{p-1} - q_1 \cdot 2^{p-2} + q_2 \cdot 2^{p-3} - q_3 \cdot 2^{p-4} + \ldots \pm q_{p-1} = 0,$$
$$3^{p-1} - q_1 \cdot 3^{p-2} + q_2 \cdot 3^{p-3} - q_3 \cdot 3^{p-4} + \ldots \pm q_{p-1} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(p-1)^{p-1} - q_1(p-1)^{p-2} + q_2(p-1)^{p-3} - q_3(p-1)^{p-4} + \ldots \pm q_{p-1} = 0.$$

Перенося въ этихъ уравненiяхъ первые члены въ первой части во вторую часть и примѣняя къ нимъ теорему Фермата, получаемъ сравненiя

$$\left.\begin{aligned}
&q_1 - q_2 + q_3 - \ldots \pm q_{p-1} \equiv 1\\
&q_1 \cdot 2^{p-2} - q_2 \cdot 2^{p-3} + q_3 \cdot 2^{p-4} - \ldots \pm q_{p-1} \equiv 1\\
&q_1 \cdot 3^{p-2} - q_2 \cdot 3^{p-3} + q_3 \cdot 3^{p-4} - \ldots \pm q_{p-1} \equiv 1\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&q_1(p-1)^{p-2} - q_2(p-1)^{p-3} + q_3(p-1)^{p-4} - \ldots \pm q_{p-1} \equiv 1
\end{aligned}\right\} \pmod{p}.$$

Обозначая теперь чрезъ m любое изъ чиселъ $1, 2, 3, \ldots p-1$, умножаемъ обѣ части каждаго изъ послѣднихъ сравненій соотвѣтственно на $1, 2^m, 3^m, \ldots (p-1)^m$, и затѣмъ складываемъ ихъ почленно; получаемъ

Обозначивъ $S_r = 1^r + 2^r + \ldots + (p-1)^r$

$$q_1 S_{p+m-2} - q_2 S_{p+m-3} + \ldots \pm q_{p-1} S_m \equiv S_m \pmod{p}.$$

если $a \equiv b$ (mod. K), $a' \equiv b'$ (mod. K), то $a + a' \equiv b + b'$ (mod. K) см. n°5 стр. 65.

гдѣ общая форма члена лѣвой части есть $(-1)^i q_{i-1} S_{p+m-i}$.

На основаніи вышедоказанной теоремы замѣчаемъ, что всѣ возможныя при разныхъ значеніяхъ m суммы въ первой части послѣдняго сравненія, за исключеніемъ одной, именно S_{p-1}, дѣлятся на p; поэтому можемъ написать

$p+m-i = p-1$, или $i = m+1$, и членъ, содержащій S_{p-1} приметъ видъ $(-1)^{m-1} q_m S_{p-1}$ и потому

$$(-1)^{m-1} q_m S_{p-1} \equiv S_m \pmod{p}.$$

Но, по той же теоремѣ, на которую только что ссылались, имѣемъ $S_{p-1} \equiv -1 \pmod{p}$; слѣдовательно

$$(-1)^m q_m \equiv S_m \pmod{p},$$

или

$$q_m \equiv (-1)^m S_m \pmod{p}.$$

такъ какъ S_{p-1} число простое съ p, то сравненіе $(-1)^{m-1} q_m S_{p-1} \equiv S_m$ (mod. p), $S_{p-1} \equiv -1$ (mod. p) можно почленно раздѣлить (см. n°16 стр. 69) и потому

Дѣлая въ этомъ сравненіи поочередно $m = 1, 2, 3, \ldots p-1$, получаемъ

$$q_1 \equiv 0,\ q_2 \equiv 0, \ldots q_{p-2} \equiv 0,\ q_{p-1} \equiv -1 \pmod{p},$$

что и слѣдовало доказать.

Въ ряду сравненій по послѣдней теоремѣ, особеннаго вниманія заслуживаетъ

$$q_{p-1} \equiv -1 \pmod{p},$$

по которому имѣемъ

(1). . . . . . $1.\ 2.\ 3 \ldots (p-1) + 1 \equiv 0 \pmod{p}$. теорема Вильсона

Весьма замѣчательно въ этомъ сравненіи то, что оно имѣетъ мѣсто только тогда, когда p число простое; при сложномъ $p = qq'$, произведеніе $1.\ 2.\ 3 \ldots (p-1)$ очевидно дѣлится на q

и сравненіе приводитъ къ невозможному, именно, что 1 дѣлится на q.

Характеристическое свойство простыхъ чиселъ, выражаемое сравненіемъ (1), извѣстно въ алгебрѣ подъ названіемъ теоремы Вильсона; оно могло бы служить критеріумомъ для узнаванія простыхъ чиселъ, еслибъ не встрѣчалось затрудненій отъ большаго числа неизбѣжныхъ дѣйствій.

Второе доказательство см. п. 36 стр. 96.; третье см. п. 97 стр. 250.

Слѣдствіе 1. *Если p число простое, то имѣетъ мѣсто тожество*

$$(x-1)(x-2)(x-3)\ldots(x-p+1)=x^{p-1}-1+pf(x),$$

гдѣ $f(x)$ изображаетъ цѣлую функцію съ цѣлыми коеффиціентами.

На самомъ дѣлѣ, внося во вторую часть тожества

$$(x-1)(x-2)(x-3)\ldots(x-p+1)=x^{p-1}-q_1x^{p-2}$$
$$+q_2x^{p-3}-\ldots\pm q_{p-1}$$

на мѣсто чиселъ $q_1, q_2, \ldots$ ихъ выраженія по формуламъ

$$q_1=a_1p,\quad q_2=a_2p,\ldots q_{p-2}=a_{p-2}p,\quad q_{p-1}=-1+a_{p-1}p,$$

гдѣ $a_1, a_2, \ldots a_{p-1}$ суть цѣлыя числа, и называя для сокращенія

$$f(x)=-a_1x^{p-2}+a_2x^{p-3}-\ldots\pm a_{p-1},$$

получаемъ требуемое равенство.

Слѣдствіе 2. *Если p число простое нечетное, то имѣетъ мѣсто тожество*

$$(x-1^2)(x-2^2)(x-3^2)\ldots\left(x-\left(\frac{p-1}{2}\right)^2\right)=x^{\frac{p-1}{2}}-1+pf_1(x),$$

гдѣ $f_1(x)$ изображаетъ функцію цѣлую съ цѣлыми коеффиціентами.

Дѣйствительно, перемножая почленно рядъ тожествъ

$$(x-1)(x-p+1)=x^2-1-p(x-1),$$

$$(x-2)(x-p+2)=x^2-2^2-p(x-2),$$

. . . .

. . . .

$$\left(x-\frac{p-1}{2}\right)\left(x-\frac{p+1}{2}\right)=x^2-\left(\frac{p-1}{2}\right)^2-p\left(x-\frac{p-1}{2}\right),$$

получаемъ

$$(x-1)(x-2)(x-3)\ldots(x-p+1)$$
$$=(x^2-1^2)(x^2-2^2)(x^2-3^2)\ldots\left(x^2-\left(\frac{p-1}{2}\right)^2\right)+p\varphi(x),$$

гдѣ $\varphi(x)$ изображаетъ для сокращенія нѣкоторую цѣлую функцію съ цѣлыми коеффиціентами.

Вкося на мѣсто первой части въ послѣднемъ тожествѣ соотвѣтствующее выраженіе по предыдущей формулѣ, получаемъ

$$(x^2-1^2)(x^2-2^2)\ldots\left(x^2-\left(\frac{p-1}{2}\right)^2\right)=x^{p-1}-1+p\left(f(x)-\varphi(x)\right).$$

Отсюда видно, что разность $f(x)-\varphi(x)$ содержитъ только члены съ четными показателями[x)]; вслѣдствіе этого можемъ для сокращенія написать

$$f(x)-\varphi(x)=f_1(x^2),$$

изображая при этомъ чрезъ $f_1(x)$ нѣкоторую цѣлую функцію съ цѣлыми коеффиціентами. Наше равенство представляется въ видѣ

$$(x^2-1^2)(x^2-2^2)\ldots\left(x^2-\left(\frac{p-1}{2}\right)^2\right)=x^{p-1}-1+pf_1(x^2),$$

Подставляя здѣсь въ обѣихъ частяхъ x на мѣсто x^2, получаемъ

$$(2)\quad (x-1^2)(x-2^2)\ldots\left(x-\left(\frac{p-1}{2}\right)^2\right)=x^{\frac{p-1}{2}}-1+pf_1(x).$$

x) ибо лѣвая часть содержитъ x только въ четныхъ степеняхъ.

Слѣдствіе 3. *Если p число простое нечетное, то произведеніе* $\left(1.\ 2.\ 3\ldots\frac{p-1}{2}\right)^2$ *сравнимо по модулю p съ* $(-1)^{\frac{p+1}{2}}$.

Предложеніе это выводится изъ (2), дѣлая $x = 0$. Оно очевидно равносильно теоремѣ Вильсона.

Итакъ, соотвѣтственно тому, будетъ ли число p формы $4n + 1$ или $4n + 3$, будетъ имѣть мѣсто одно изъ двухъ:

(3)....... $\left(1.\ 2.\ 3\ldots\frac{p-1}{2}\right)^2 \equiv -1 \pmod{p}$

или

(4)....... $\left(1.\ 2.\ 3\ldots\frac{p-1}{2}\right)^2 \equiv 1 \pmod{p}$.

Слѣдствіе 4. *Если p число простое вида $4n + 3$, то произведеніе* $1.\ 2.\ 3\ldots\frac{p-1}{2}$ *сравнимо съ однимъ изъ чиселъ* ± 1, *и наоборотъ.*

Это обнаруживается непосредственно, если сравненіе (4) написать въ другомъ видѣ, именно:

умножение сравнений см. n°7 стр. 65.

$$\left[1.\ 2.\ 3\ldots\frac{p-1}{2} - 1\right]\left[1.\ 2.\ 3\ldots\frac{p-1}{2} + 1\right] \equiv 0 \pmod{p}.$$

Не менѣе ясно и то, что произведеніе $1.\ 2.\ 3\ldots\frac{p-1}{2}$ не можетъ быть сравнимо ни съ -1 ни съ $+1$, если p есть вида $4n + 1$; на это прямо указываетъ сравненіе (3).

Испытывая поочередно различныя простыя числа, получаемъ слѣдующую таблицу для абсолютно малыхъ вычетовъ r произведенія $1.\ 2.\ 3\ldots\frac{p-1}{2}$.

$p = 4n + 1$,	r	$p = 4n + 3$,	r
5	2	3	+1
13	5	7	—1
17	—4	11	—1
29	12	19	—1
37	—6	23	+1
41	9	31	+1

$p=4n+1$,	r	$p=4n+3$,	r
53	23	43	—1
61	11	47	—1
73	27	59	+1
89	34	67	—1
97	22	71	+1
101	—10	79	—1
113		83	+1
137			

35. Съ помощью одного изъ предыдущихъ сравненій легко доказать знаменитую теорему Фермата, относящуюся къ простымъ числамъ вида $4n+1$. Но начнемъ съ доказательства слѣдующей леммы.

Всякое простое число вида 4n+1 разлагается на сумму двухъ квадратовъ.

Лемма. *Всякій дѣлитель суммы двухъ взаимно простыхъ квадратовъ самъ разлагается на сумму двухъ квадратовъ.*

На основаніи извѣстнаго тожества

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$$

мы заключаемъ, что произведеніе какого угодно числа цѣлыхъ множителей, изъ коихъ каждый есть сумма двухъ квадратовъ, разлагается на сумму двухъ квадратовъ. Слѣдовательно при доказательствѣ леммы мы въ правѣ ограничиться предположеніемъ, что разсматриваемый дѣлитель простой.[x] Можно предположить еще, что онъ >2, ибо число 2 есть очевидно сумма двухъ квадратовъ 1^2+1^2.

Пусть p означаетъ простой нечетный дѣлитель суммы a^2+b^2, при чемъ числа a и b относительно простыя. Въ уравненіи

$$(1) \quad \ldots\ldots\ldots\ldots \quad a^2+b^2=pq$$

слѣдуетъ предполагать $q>1$, ибо при $q=1$ справедливость леммы очевидна.

Мы покажемъ, что съ помощью равенства (1) можно составить другое равенство $c^2+d^2=pq'$ такого же вида какъ (1),

x) такъ какъ, если мы докажемъ, что каждый изъ простыхъ дѣлителей $p_1, p_2, \ldots, p_n$ разлагается на сумму двухъ квадратовъ, то можно будетъ утверждать, что любое изъ произведеній этихъ дѣлителей также разлагается на сумму двухъ квадратовъ.

но въ которомъ коэффиціентъ q' будетъ меньше q. Уменьшая такимъ образомъ послѣдовательно коэффиціентъ во второй части, мы, очевидно, дойдемъ до такого равенства, въ которомъ этотъ коэффиціентъ будетъ равенъ 1, и слѣдовательно лемма будетъ доказана, такъ какъ p окажется разложеннымъ на сумму двухъ квадра[тов].

1. Допустивъ сперва, что въ (1) одно изъ чиселъ a и b или оба больше $\frac{p}{2}$. Въ такомъ случаѣ составляемъ абсолютно малые вычеты чиселъ a и b по модулю p. Обозначивъ ихъ числовыя величины чрезъ a' и b', имѣемъ

$$a' < \frac{p}{2}, \quad b' < \frac{p}{2},$$

$$a' \equiv \pm a \ (\text{mod.}\, p); \quad b' \equiv \pm b \ (\text{mod.}\, p).$$

Возвышая обѣ части каждаго изъ этихъ сравненій въ квадратъ и затѣмъ складывая ихъ почленно, получаемъ

$$a'^2 + b'^2 \equiv a^2 + b^2 \ (\text{mod.}\, p);$$

отсюда заключаемъ

$$a'^2 + b'^2 \equiv 0 \ (\text{mod.}\, p),$$

вслѣдствіе чего можно написать

$$(2) \ldots\ldots\ldots\ldots\ldots \quad a'^2 + b'^2 = pq'.$$

Здѣсь $q' < q$; ибо по предположенію по крайней мѣрѣ одно изъ чиселъ a, b больше своего абсолютно малаго вычета, что приводитъ къ неравенству $a^2 + b^2 > a'^2 + b'^2$,x) или $pq > pq'$, а это по сокращеніи на p даетъ $q > q'$.

Легко также убѣдиться, что q' не равно нулю. Въ противномъ случаѣ мы имѣли бы $a' = b' = 0$, а это приводитъ къ сравненіямъ

$$a \equiv 0, \quad b \equiv 0 \ (\text{mod.}\, p),$$

что невозможно, ибо a и b относительно простыя.

---

x) при $a > \frac{p}{2}$ будетъ minim. $a = \frac{p+1}{2}$, а maxim $a' = \frac{p-1}{2}$; поэтому minim. $(a^2 - a'^2) = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$ [illegible]
при $b < \frac{p}{2}$ будетъ $b \leq \frac{p-1}{2}$ и $b' = b$; поэтому [illegible] измѣненіи b отъ $+\frac{p-1}{2}$ до $-\frac{p-1}{2}$ [illegible]
[illegible] равно 0; отсюда minim $[(a^2 - a'^2) + (b^2 - b'^2)] = p$; поэтому въ [illegible]
[illegible] $\geq p$ [illegible] или $q' < q - 1$.

Изображая чрезъ λ общій наибольшій дѣлитель чиселъ a' и b', мы замѣчаемъ, что λ не дѣлится на p; ибо допустивъ противное, мы имѣли бы сравненія $a' \equiv b' \equiv 0 \pmod{p}$, откуда вытекаетъ

$$a \equiv b \equiv 0 \pmod{p},$$

что невозможно.

Вторая часть равенства (2) дѣлится на λ^2, а такъ какъ λ и p относительно простыя, то слѣдовательно q' дѣлится на λ^2. Полагая

$$a' = \lambda a'', \quad b' = \lambda b'', \quad q' = \lambda^2 q'',$$

вносимъ эти выраженія въ (2), и затѣмъ сокращаемъ обѣ части на λ^2; получаемъ

$$(3) \ldots\ldots\ldots\ldots \quad a''^2 + b''^2 = pq''.$$

Въ равенствѣ этомъ a'' и b'' относительно простыя, что касается коеффиціента q'', то

$$q'' \leqq q' < q.$$

Слѣдовательно въ разсматриваемомъ случаѣ, когда въ (1) одно изъ чиселъ a, b или оба $> \frac{p}{2}$, возможность пониженія коеффиціента q доказана.

2. Переходимъ ко второму случаю, когда оба числа a и b меньше $\frac{p}{2}$. Прежде всего отмѣтимъ неравенство

$$a^2 + b^2 < \frac{p^2}{2},$$

или

$$pq < \frac{p^2}{2},$$

откуда получаемъ

$$(4) \ldots\ldots\ldots\ldots \quad q < \frac{p}{2}.$$

Обозначая чрезъ a_1 и b_1 абсолютно малые вычеты чиселъ a и b, составленные по модулю q, имѣемъ

$$a_1 \leqq \frac{q}{2}, \quad b_1 \leqq \frac{q}{2},$$

$$a \equiv a_1, \quad b \equiv b_1 \pmod{q}.$$

Отсюда выводимъ

$$a_1^2 + b_1^2 \equiv a^2 + b^2 \equiv 0 \pmod{q},$$

вслѣдствіе чего можно написать

(5) . . . . $a_1^2 + b_1^2 = qq_1,$

при чемъ имѣемъ

$$qq_1 \leqq \frac{q^2}{4} + \frac{q^2}{4},$$ ибо $a_1 \leqq \frac{q}{2}$ и $b_1 \leqq \frac{q}{2}$.

откуда заключаемъ

(6). . . . . $q_1 \leqq \frac{q}{2}.$

Съ другой стороны, коеффиціентъ q_1 не равенъ нулю. Ибо допустивъ $q_1 = 0$ мы имѣли бы уравненіе $a_1^2 + b_1^2 = 0$, откуда вытекаетъ

$$a_1 = b_1 = 0,$$

а это приводитъ къ сравненію

$$a \equiv b \equiv 0 \pmod{q},$$

что невозможно.

Принимая къ свѣдѣнію вышесказанное, перемножаемъ теперь почленно равенства (1) и (5); получаемъ

$$(a^2 + b^2)(a_1^2 + b_1^2) = pq^2q_1,$$

или

$$(aa_1 + bb_1)^2 + (ab_1 - a_1b)^2 = pq^2q_1.$$

Такъ какъ $a_1 \equiv a$ и $b_1 \equiv b \pmod{q}$, то слѣдовательно

$$aa_1 + bb_1 \equiv a^2 + b^2 \equiv 0 \pmod{q},$$ ибо $a^2 + b^2 = pq$.

$$ab_1 - a_1b \equiv 0 \pmod{q},$$

и поэтому можно написать

$$aa_1 + bb_1 = qc,$$

$$ab_1 - a_1b = qd.$$

Вносимъ эти выраженія въ первую часть предыдущаго равенства и затѣмъ сокращаемъ обѣ части на q^2; получаемъ

(7) . . . . $c^2 + d^2 = pq_1$.

Изображая чрезъ μ общій наибольшій дѣлитель чиселъ c и d, мы замѣчаемъ, что μ не дѣлится на p. Ибо допустивъ противное мы имѣли бы два сравненія

$$c \equiv d \equiv 0 \ (\text{mod.}\, p),$$

которыя приводятъ къ такимъ:

$$\left.\begin{array}{l} aa_1 + bb_1 \equiv 0 \\ ab_1 - a_1 b \equiv 0 \end{array}\right\} (\text{mod.}\, p).$$

Умножая обѣ части перваго изъ нихъ на a_1, втораго на b_1, и затѣмъ складывая, получаемъ

$$a(a_1^2 + b_1^2) \equiv 0 \ (\text{mod.}\, p).$$

Но a есть число простое съ p; поэтому послѣднее сравненіе можно сократить на a, послѣ чего получаемъ

$$a_1^2 + b_1^2 \equiv 0 \ (\text{mod.}\, p),$$

или

$$qq_1 \equiv 0 \ (\text{mod.}\, p),$$

сравненіе невозможное; ибо $q < \frac{p}{2}$, а q_1, будучи $\leqq \frac{q}{2}$, тѣмъ самымъ $< \frac{p}{4}$.

Итакъ, числа μ и p относительно простыя. Отсюда слѣдуетъ, если принять во вниманіе (7), что q_1 дѣлится на μ^2. Полагая

$$c = c'\mu, \quad d = d'\mu, \quad q_1 = q'_1 \mu^2,$$

изъ (7) выводимъ

(8) . . . . $c'^2 + d'^2 = pq'_1$.

Если $\mu = 1$, послѣднее равенство не отличается тогда отъ (7). Во всякомъ случаѣ имѣемъ

$$q'_1 \leqq q_1 \leqq \frac{q}{2},$$

при этомъ числа c' и d' относительно простыя; слѣдовательно
Доказана и въ этомъ случаѣ возможность пониженія коэффиціента q;
равенство (8) удовлетворяетъ требуемымъ условіямъ, и такимъ образомъ лемма доказана вполнѣ.[x)]

Съ ея помощью доказывается очень просто вышеупомянутая теорема Фермата, которая состоитъ въ слѣдующемъ.

Теорема. *Всякое простое число вида $4n + 1$ разлагается на сумму двухъ квадратовъ.*

Дѣйствительно, сравненіе (3) предыдущаго номера показываетъ, что простое число p вида $4n + 1$ есть дѣлитель суммы двухъ квадратовъ

$$\left(1.\ 2.\ 3\ldots\frac{p-1}{2}\right)^2 + 1,$$

отсюда, на основаніи предыдущей леммы, заключаемъ, что p разлагается на сумму двухъ квадратовъ.

Новое доказательство теоремы Вильсона.

36. Въ заключеніе настоящаго параграфа мы укажемъ на одну формулу, хорошо извѣстную въ анализѣ, съ помощью которой теорему Вильсона выводимъ почти непосредственно, но все-таки принимая теорему Фермата за извѣстную.

Подставляя въ обѣихъ частяхъ тожества

$$(x+1)^n - x^n = nx^{n-1} + \frac{n(n-1)}{1.2}x^{n-2} + \ldots + 1$$

$x + 1$ на мѣсто x и изъ полученнаго такимъ образомъ новаго тожества вычитая почленно предыдущее, получаемъ

$$(x+2)^n - 2(x+1)^n + x^n = n(n-1)x^{n-2} + p_1 x^{n-3} + \ldots,$$

гдѣ $p_1, p_2, \ldots$ изображаютъ цѣлые коэффиціенты, выраженія которыхъ нѣтъ надобности составлять.

x) Значитъ всякій [illegible] двухъ взаимно простыхъ [illegible] разлагается на простые множители вида суммы двухъ квадратовъ, т.е. вида $4n+1$.

Подставляя въ обѣихъ частяхъ послѣдняго тожества $x+1$ на мѣсто x, и изъ полученнаго такимъ образомъ тожества вычитая предыдущее, находимъ

$$(x+3)^n - 3(x+2)^n + 3(x+1)^n - x^n$$
$$= n(n-1)(n-2)x^{n-3} + qx^{n-4} + \ldots$$

Послѣ повторенія $(m-1)$ разъ подобной операціи, находимъ

$$(x+m)^n - \frac{m}{1}(x+m-1)^n + \frac{m(m-1)}{1.2}(x+m-2)^n - \ldots$$
$$+ (-1)^m x^m = n(n-1)(n-2)\ldots(n-m+1)x^{n-m}$$
$$+ ax^{n-m-1} + \ldots,$$

гдѣ $a, \ldots$ изображаютъ цѣлые коеффиціенты.

Для насъ особенно важенъ частный случай, когда $m = n$; тогда имѣемъ

$$(x+n)^n - \frac{n}{1}(x+n-1)^n + \frac{n(n-1)}{1.2}(x+n-2)^n + \ldots$$
$$+ (-1)^n x^n = 1.\ 2.\ 3 \ldots n.$$

Это именно и есть та формула, на которую мы желали указать. Дѣлая въ ней $x = 0$, $n = p-1$, получаемъ

$$(p-1)^{p-1} - \frac{p-1}{1}(p-2)^{p-1} + \frac{(p-1)(p-2)}{1.2}(p-3)^{p-1} - \ldots$$
$$+ (-1)^{p-2}\frac{p-1}{1}1^{p-1} = 1.\ 2.\ 3 \ldots (p-1).$$

Допустивъ теперь, что число p есть простое, и принимая во вниманіе теорему Фермата, имѣемъ

$$(p-1)^{p-1} \equiv 1,\ (p-2)^{p-1} \equiv 1,\ (p-3)^{p-1} \equiv 1, \ldots$$
$$1^{p-1} \equiv 1 \pmod{p},$$

вслѣдствіе чего послѣднее равенство приводитъ къ сравненію

$$1.\ 2.\ 3 \ldots (p-1) \equiv 1 - \frac{p-1}{1} + \frac{(p-1)(p-2)}{1.2} - \ldots$$
$$- \frac{p-1}{1} \pmod{p}.$$

По извѣстному свойству коеффиціентовъ въ биномѣ Ньютона вторая часть послѣдняго сравненія равна -1; слѣдовательно

$$1.\,2.\,3\ldots(p-1)\equiv -1\ (\mathrm{mod.}\,p),$$

что и требовалось показать.

§ V. Рѣшеніе сравненій первой степени.

Общія замѣчанія.

37. Въ теоріи чиселъ разсматриваются сравненія вида

$$(1)\quad Ax^n + A_1x^{n-1} + \ldots + A_{n-1}x + A_n \equiv 0\ (\mathrm{mod.}\,k),$$

гдѣ A, A_1,... какіе нибудь цѣлые коеффиціенты, x неизвѣстное цѣлое число.

Если коеффиціенты A, A_1, A_2,... соотвѣтственно сравнимы по модулю k съ числами A', A'_1, A'_2,..., то сравненіе

$$(2)\quad A'x^n + A'_1x^{n-1} + \ldots + A'_{n-1}x + A'_n \equiv 0\ (\mathrm{mod.}\,k)$$

равносильно сравненію (1), то есть, всякое число x, удовлетворяющее одному изъ сравненій (1) или (2) будетъ удовлетворять и остальному. Поэтому сравненія (1) и (2) не слѣдуетъ считать за различныя, и всегда можно предполагать, что въ данномъ сравненіи всѣ коеффиціенты положительны и меньше модуля или, что числовыя ихъ величины не превышаютъ половины модуля.

Степень сравненія опредѣляется наивысшею степенью неизвѣстнаго x, у которой коеффиціентъ не дѣлится на модуль; такъ, напримѣръ, степень сравненія

$$14x^7 - 7x^5 - 2x^2 + 3 \equiv 0\ (\mathrm{mod.}\,7)$$

есть 2.

Если число $x = a$ удовлетворяетъ сравненію (1), то и всѣ числа, сравнимыя съ a по модулю k, также будутъ удовлетво-

рять тому же сравненію. Такія рѣшенія не считаются за различныя; напротивъ, два числа, удовлетворяющія сравненію (1), но не сравнимыя между собою по модулю k, считаются за различныя рѣшенія. Отсюда вытекаетъ, что число рѣшеній какого угодно сравненія равняется числу чиселъ въ ряду

$$0,\ 1,\ 2, \ldots k-2,\ k-1,$$

удовлетворяющихъ ему. т. е. не более k.

Напримѣръ, сравненіе

$$x^7 + x^6 + 2x^5 - 3x^4 - 4x^3 + 2x^2 + 3x + 2 \equiv 0 \pmod{11}$$

имѣетъ всего три рѣшенія, именно:

$$x \equiv 3,\ 8,\ 10 \pmod{11},$$

или, что одно и то же,

$$x \equiv 3,\ -3,\ -1 \pmod{11}.$$

Рѣшенія сравненія называютъ также его *корнями*.

Сравненіе называется *тожественнымъ*, когда всѣ коэффиціенты его дѣлятся на модуль; тогда всякое цѣлое число удовлетворяетъ сравненію. Однако нельзя утверждать обратно: по теоремѣ Фермата сравненію

$$x^p - x \equiv 0 \pmod{p},$$

при p простомъ, удовлетворяетъ всякое цѣлое число, между тѣмъ оно не есть тожество.

38. Переходя къ сравненіямъ первой степени, начнемъ съ доказательства слѣдующей основной теоремы. Доказательство основной теоремы.

Теорема. *Если числа a и k относительно простыя, то сравненіе*

$$ax \equiv b \pmod{k}$$

имѣетъ одно и только одно рѣшеніе.

Нѣтъ никакого труда доказать напередъ невозможность существованія двухъ рѣшеній. На самомъ дѣлѣ, допустимъ, что два числа x_1 и x_2 удовлетворяютъ означенному сравненію; имѣемъ

$$\left.\begin{aligned} ax_1 &\equiv b \\ ax_2 &\equiv b \end{aligned}\right\} (\text{mod. } k),$$

откуда посредствомъ вычитанія выводимъ

$$a(x_2 - x_1) \equiv 0 \ (\text{mod. } k).$$

Обѣ части этого сравненія можно сократить на a, послѣ чего получаемъ

$$x_2 - x_1 \equiv 0 \ (\text{mod. } k),$$

или

$$x_2 \equiv x_1 \ (\text{mod. } k).$$

Это показываетъ, что рѣшеніе x_2 не отличается отъ x_1.

Итакъ, намъ остается доказать существованіе одного рѣшенія. Это дѣлается легко на разные способы.

Первое доказательство. Составляемъ произведенія

$$0, a, 2a, 3a, \ldots (k-1)a$$

и называемъ соотвѣтствующіе имъ наименьшіе положительные вычеты чрезъ

(1) . . . . $r_0, r_1, r_2, r_3, \ldots r_{k-1}$.

Всѣ числа въ послѣднемъ ряду различны. Дѣйствительно, если допустимъ, что $r_i = r_j$ при различныхъ значкахъ i и j, то получаемъ сравненіе

$$ia \equiv ja \ (\text{mod. } k),$$

которое по сокращенію на a приводится къ такому:

$$i - j \equiv 0 \ (\text{mod. } k),$$

а это невозможно, ибо оба числа i и j меньше k.

Отсюда слѣдуетъ, что рядъ (1) представляетъ нѣкоторое перемѣщеніе чиселъ $0, 1, 2, \ldots k-1$, и потому между числами (1) находится одно и только одно, которое сравнимо съ b по модулю k. Пусть это число есть r_α; имѣемъ

$$b \equiv r_\alpha \pmod{k},$$

$$a\alpha \equiv r_\alpha \pmod{k},$$

откуда выводимъ

$$a\alpha \equiv b \pmod{k}.$$

Число α удовлетворяетъ данному сравненію.

Второе доказательство. Такъ какъ по предположенію общій наибольшій дѣлитель чиселъ a и k равенъ 1, то можно найти два цѣлыхъ числа u и v удовлетворяющихъ уравненію

$$au + kv = 1.$$

Это было доказано въ началѣ первой главы. см. п. 3 стр. 4.

Умножая обѣ части послѣдняго равенства на b, получаемъ

$$abu + kbv = b,$$

отсюда вытекаетъ сравненіе

$$abu \equiv b \pmod{k},$$

которое показываетъ, что bu удовлетворяетъ данному сравненію.

Третье доказательство. По теоремѣ Эйлера имѣемъ см. стр. 76

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

Отсюда, умножая обѣ части на b, получаемъ

$$ba^{\varphi(k)} \equiv b \pmod{k}.$$

Вслѣдствіе этого сравненіе

$$ax \equiv b \pmod{k}$$

оказывается равносильнымъ сравненію

$$ax \equiv ba^{\varphi(k)} \pmod{k},$$

а это послѣднее по сокращеніи на a приводится къ такому

$$x \equiv ba^{\varphi(k)-1} \pmod{k},$$

которому очевидно удовлетворяетъ всякое число, сравнимое по модулю k съ произведеніемъ

$$ba^{\varphi(k)-1}.$$

Число решений какого угодно сравнения первой степени.

39. Покажемъ теперь, какъ опредѣляются рѣшенія сравненія

$$(1) \;\ldots\ldots\ldots\ldots\; ax \equiv b \pmod{k}$$

въ томъ случаѣ, когда общій наибольшій дѣлитель d чиселъ a и k больше 1.

Если b не дѣлится на d, сравненіе не имѣетъ вовсе рѣшеній, ибо по свойству сравнимыхъ чиселъ всякій общій дѣлитель чиселъ a и k долженъ дѣлить b.

Допустимъ, что b дѣлится на d. Въ такомъ случаѣ мы можемъ сравненіе (1) замѣнить слѣдующимъ, равносильнымъ ему:

$$(2) \;\ldots\ldots\ldots\; \frac{a}{d}\, x \equiv \frac{b}{d} \left(\text{mod.}\ \frac{k}{d}\right),$$

которое подходитъ подъ случай, разобранный въ предыдущемъ номерѣ; ибо числа $\frac{a}{d}$ и $\frac{k}{d}$ относительно простыя.

Изображая чрезъ α число, удовлетворяющее (2), имѣемъ формулу

$$(3) \;\ldots\ldots\ldots\ldots\; x = \alpha + \frac{k}{d}\, t,$$

которая даетъ всѣ числа, удовлетворяющія сравненію (1); при этомъ перемѣнное t принимаетъ всякія цѣлыя значенія.

Чтобъ два значенія x составляли дѣйствительно различныя рѣшенія сравненія (1) достаточно и необходимо, чтобы соотвѣт-

ствующія имъ значенія перемѣннаго t были несравнимы между собою по модулю d. Дѣйствительно, если допустимъ, что $t_1 \equiv t_2$ (mod. d), то отсюда получаемъ

$$\frac{k}{d} t_1 \equiv \frac{k}{d} t_2 \ (\text{mod. } k);$$

прибавляя къ обѣимъ частямъ по α, имѣемъ

$$\alpha + \frac{k}{d} t_1 \equiv \alpha + \frac{k}{d} t_2 \ (\text{mod. } k)$$

или

$$x_1 \equiv x_2 \ (\text{mod. } k).$$

Наоборотъ, изъ послѣдняго сравненія, слѣдуя обратнымъ порядкомъ, приходимъ къ сравненію $t_1 \equiv t_2$ (mod. d).

Итакъ, чтобы изъ (3) получить всѣ рѣшенія сравненія (1), стоитъ только для t давать послѣдовательно значенія, составляющія полную систему чиселъ несравнимыхъ по модулю d, напримѣръ, $t = 0, 1, 2, \ldots d - 1$.

Отсюда получаемъ теорему.

Теорема. *Если общій наибольшій дѣлитель d чиселъ a и k дѣлитъ b, то сравненіе*

$$ax \equiv b \ (\text{mod. } k)$$

имѣетъ ровно d рѣшеній; всѣ они опредѣляются помощью одного изъ нихъ α по слѣдующимъ формуламъ:

$$x \equiv \alpha, \ x_1 \equiv \alpha + \frac{k}{d}, \ x_2 \equiv \alpha + 2\frac{k}{d}, \ldots$$

$$x_{d-1} \equiv \alpha + (d-1)\frac{k}{d} \ (\text{mod. } d).$$

Примѣръ. Опредѣлить рѣшенія сравненія

$$20x \equiv 28 \ (\text{mod. } 132).$$

Раздѣляя обѣ части сравненія и модуль на $d = 4$, получаемъ сравненіе

$$5x \equiv 7 \ (\text{mod. } 33).$$

По одному изъ трехъ вышеуказанныхъ способовъ находимъ рѣшеніе послѣдняго сравненія $x = 8$. Отсюда прямо находимъ всѣ рѣшенія даннаго сравненія; ихъ всего четыре:

$$x \equiv 8,\ 41,\ 74,\ 107\ (\text{mod. } 132).$$

Рѣшеніе нѣсколькихъ совокупныхъ сравненій первой степени съ различными модулями.

40. Теперь мы можемъ показать способъ нахожденія всѣхъ чиселъ x, удовлетворяющихъ одновременно нѣсколькимъ сравненіямъ такого вида:

$$x \equiv \alpha\ (\text{mod. } a),\ \ x \equiv \beta\ (\text{mod. } b), \ldots x \equiv \gamma\ (\text{mod. } c),$$

гдѣ модули $a, b, \ldots$ равно какъ и $\alpha, \beta, \ldots$ суть какія угодно данныя числа.

Въ нѣкоторыхъ изысканіяхъ задача эта представляется существенною; сейчасъ мы покажемъ одно изъ важнѣйшихъ ея приложеній.

Переходя къ рѣшенію, мы начнемъ съ двухъ сравненій

(1) . . . . $x \equiv \alpha\ (\text{mod. } a), \quad x \equiv \beta\ (\text{mod. } b)$.

Числа, удовлетворяющія первому, опредѣляются формулой

(2) . . . . $x = \alpha + ay$.

Вставляя это выраженіе на мѣсто x во второе (1), получаемъ условіе для опредѣленія y

(3) . . . . $ay \equiv \beta - \alpha\ (\text{mod. } b)$.

Всякое число y, удовлетворяющее (3), опредѣляетъ по формулѣ (2) соотвѣтствующее число x, которое удовлетворяетъ обоимъ сравненіямъ (1).

Весь вопросъ сведенъ на рѣшеніе сравненія (3).

Если общій наибольшій дѣлитель d чиселъ a и b не дѣлитъ разности $\alpha - \beta$, сравненіе (3) не имѣетъ рѣшенія; тогда сравненія (1) находятся въ противорѣчіи между собой: задача невозможна.

Напротивъ, если разность $\alpha - \beta$ дѣлится на d, сравненіе (3) имѣетъ рѣшенія, и всѣ они получаются изъ одного y_0 по формулѣ

$$y = y_0 + \frac{b}{d}t,$$

давая для t всякія цѣлыя значенія. Слѣдовательно всѣ рѣшенія сравненій (1) получаются изъ общей формулы

$$x = \alpha + ay_0 + \frac{ab}{d}t.$$

Ихъ число, какъ видимъ, безконечно велико; но всѣ они сравнимы между собой по модулю $\frac{ab}{d}$, и если обозначить одно, любое изъ нихъ чрезъ x_0, то послѣднюю формулу можно написать такъ:

$$x \equiv x_0 \left(\text{mod. } \frac{ab}{d}\right);$$

при этомъ слѣдуетъ обратить вниманіе, что модуль $\frac{ab}{d}$ равенъ наименьшему кратному модулей a и b.

Перейдемъ теперь къ тремъ сравненіямъ

(4) . . $x \equiv \alpha$ (mod. a), $x \equiv \beta$ (mod. b), $x \equiv \gamma$ (mod. c).

Беремъ сперва два изъ нихъ, напримѣръ,

$$x \equiv \alpha \text{ (mod. } a), \quad x \equiv \beta \text{ (mod. } b),$$

и узнаемъ, имѣютъ ли они рѣшеніе или нѣтъ. Въ послѣднемъ случаѣ задача невозможна, между тѣмъ какъ въ первомъ случаѣ сравненія (4) равносильны двумъ такимъ:

$$x \equiv x_0 \left(\text{mod. } \frac{ab}{d}\right), \quad x \equiv \gamma \text{ (mod. } c).$$

Рѣшая ихъ по предыдущему способу, мы опредѣлимъ всѣ рѣшенія системы (4).

Подобнымъ образомъ слѣдуетъ поступать въ случаѣ какого угодно числа сравненій вида (1), и на основаніи вышесказаннаго заключаемъ слѣдующее.

Теорема. *Рѣшеніе сравненія какой угодно степени* $f(x) \equiv 0 \pmod{k}$ *со сложнымъ модулемъ* $k = p^\alpha q^\beta . . . r^\gamma$ *приводится къ рѣшенію нѣсколькихъ отдѣльныхъ сравненій*

$$f(x) \equiv 0 \pmod{p^\alpha},\quad f(x) \equiv 0 \pmod{q^\beta}, . . . f(x) \equiv 0 \pmod{r^\gamma},$$

модули которыхъ суть степени простыхъ чиселъ. Число рѣшеній начальнаго сравненія равно произведенію чиселъ, показывающихъ сколько рѣшеній имѣетъ каждое изъ послѣднихъ.

Въ самомъ дѣлѣ, всякое число x, удовлетворяющее сравненію

$$(1) \;. . . . . \; f(x) \equiv 0 \pmod{p^\alpha q^\beta . . . r^\gamma}$$

удовлетворяетъ каждому изъ сравненій

$$(2) \;. . . . . \left\{\begin{array}{l} f(x) \equiv 0 \pmod{p^\alpha}, \\ f(x) \equiv 0 \pmod{q^\beta}, \\ . . . . \\ . . . . \\ f(x) \equiv 0 \pmod{r^\gamma}, \end{array}\right.$$

и наоборотъ, всякое число x, удовлетворяющее каждому изъ сравненій (2), удовлетворяетъ также (1).

Если, слѣдовательно, одно какое либо (2) не имѣетъ рѣшенія, то сравненіе (1) невозможно.

Допустимъ, вообще, что сравненіе $f(x) \equiv 0 \pmod{p^\alpha}$ имѣетъ m рѣшеній, и обозначимъ ихъ чрезъ $a_1, a_2, . . . a_m$; что сравненіе $f(x) \equiv 0 \pmod{q^\beta}$ имѣетъ m' рѣшеній, и обозначимъ ихъ чрезъ $b_1, b_2, . . . b_{m'}$, и такъ далѣе. Всякое число x, удовлетворяющее одновременно сравненіямъ (2), будетъ очевидно удовлетворять сравненіямъ

$$(3) \;. . . . . \left\{\begin{array}{l} x \equiv a_i \pmod{p^\alpha}, \\ x \equiv b_j \pmod{q^\beta}, \\ . . . . \\ . . . . \\ x \equiv c_l \pmod{r^\gamma}, \end{array}\right.$$

гдѣ a_i изображаетъ одно изъ чиселъ $a_1, a_2, \ldots a_m$, b_j — одно изъ чиселъ $b_1, b_2, \ldots b_{m'}$ и т. д. Наоборотъ, если a_i изображаетъ любое число въ ряду $a_1, a_2, \ldots a_m$, b_j — любое число въ ряду $b_1, b_2, \ldots b_{m'}$ и т. д., то всякое число, удовлетворяющее сравненіямъ (3) будетъ удовлетворять всѣмъ сравненіямъ (2), а тѣмъ самымъ и (1).

Итакъ, каждое рѣшеніе сравненія (1) есть рѣшеніе системы вида (3), и наоборотъ. Различнымъ рѣшеніямъ сравненія (1) соотвѣтствуютъ различныя системы $a_i, b_j, \ldots c_l$; поэтому число рѣшеній начальнаго сравненія равняется числу всѣхъ означенныхъ системъ, что въ свою очередь равно произведенію $m\, m' \ldots$ Теорема такимъ образомъ дѣлается очевидной.

Примѣръ. Требуется найти всѣ рѣшенія сравненія

$$x^2 - 7x + 1 \equiv 0 \pmod{45}.$$

Для этого ищемъ сперва рѣшеній сравненія

$$x^2 - 7x + 1 \equiv 0 \pmod{5},$$

которыя, замѣтимъ, получаются здѣсь непосредственно, ибо сравненіе можно написать такъ:

$$(x - 1)^2 \equiv 0 \pmod{5},$$

откуда видно, что существуетъ одно только рѣшеніе $x = 1$.

Переходимъ затѣмъ къ сравненію

$$x^2 - 7x + 1 \equiv 0 \pmod{9};$$

оно также рѣшается непосредственно; стоитъ только написать его такъ:

$$(x + 1)^2 \equiv 0 \pmod{9};$$

отсюда видно, что существуютъ два рѣшенія и не болѣе, именно, $x = -1$ и $x = 2$.

Рѣшаемъ теперь по извѣстному намъ способу совокупную систему

$$x \equiv 1 \text{ (mod. 5)}, \quad x \equiv -1 \text{ (mod. 9)};$$

находимъ

$$x \equiv -19 \text{ (mod. 45)}.$$

Это одно рѣшеніе даннаго сравненія.

Рѣшаемъ вторую систему сравненій

$$x \equiv 1 \text{ (mod. 5)}, \quad x \equiv 2 \text{ (mod. 9)};$$

находимъ

$$x \equiv 11 \text{ (mod. 45)}.$$

Это второе рѣшеніе даннаго сравненія.

Другихъ рѣшеній, кромѣ найденныхъ двухъ, не существуетъ.

§ VI. Рѣшеніе нѣсколькихъ совокупныхъ сравненій первой степени.

Приведеніе къ простѣйшему виду.

43. Обозначивъ для сокращенія чрезъ $u_1, u_2, u_3, \ldots u_n$ линейныя функціи

$$u_1 = a_{1,1} x_1 + a_{1,2} x_2 + \ldots + a_{1,n} x_n + b_1,$$

$$u_2 = a_{2,1} x_1 + a_{2,2} x_2 + \ldots + a_{2,n} x_n + b_2,$$

. . . .

. . . .

$$u_n = a_{n,1} x_1 + a_{n,2} x_2 + \ldots + a_{n,n} x_n + b_n,$$

въ которыхъ коэффиціенты $a_{1,1}, \ldots a_{n,n}$ равно какъ и послѣдніе члены $b_1, b_2, \ldots b_n$ суть цѣлыя числа, — мы предлагаемъ себѣ найти цѣлыя числа $x_1, x_2, \ldots x_n$, удовлетворяющія слѣдующей системѣ сравненій:

(1). . . . . $u_1 \equiv 0, \ u_2 \equiv 0, \ldots u_n \equiv 0 \text{ (mod. } k).$

Для этого мы сдѣлаемъ нѣсколько предварительныхъ замѣчаній.

Очевидно, что изъ системы (1) можно выводить на разные способы новыя системы линейныхъ сравненій, которымъ будутъ удовлетворять всѣ рѣшенія системы (1); пусть одна изъ такихъ системъ будетъ

$$\textbf{(2)} \ldots\ldots v_1 \equiv 0,\ v_2 \equiv 0, \ldots v_n \equiv 0 \ (\mathrm{mod.}\ k).$$

Новая система (2) не всегда можетъ быть считаемой за равносильную съ (1); для равносильности необходимо доказать, что всякое рѣшеніе системы (2) удовлетворяетъ также и (1).

Двѣ системы сравненій, равносильныя съ нѣкоторой третьей системой, равносильны между собой.

Каждый изъ коеффиціентовъ $a_{i,k}$, равно какъ и каждый изъ извѣстныхъ членовъ b_i, въ системѣ (1) можно замѣнить числомъ сравнимымъ съ нимъ по модулю k; полученная вслѣдствіе этого новая система очевидно есть равносильная съ первоначальной.

Можно также обѣ части каждаго изъ сравненій (1) умножить на любое число простое съ k; полученная новая система будетъ очевидно равносильною съ первоначальной.

Наконецъ легко замѣтить, что на мѣсто какого нибудь сравненія въ системѣ (1), напримѣръ $u_i \equiv 0$ (mod. k), можно подставить сравненіе $u_i - mu_j \equiv 0$ (mod. k), при чемъ j не равно i; полученная новая система будетъ равносильною съ первоначальной.

Относительно послѣдней подстановки слѣдуетъ сдѣлать два замѣчанія: во первыхъ, она не измѣняетъ значенія опредѣлителя данной системы

$$\Delta = \begin{vmatrix} a_{1,1} & a_{1,2} \ldots a_{1,n} \\ a_{2,1} & a_{2,2} \ldots a_{2,n} \\ \ldots & \ldots\ldots \\ \ldots & \ldots\ldots \\ a_{n,1} & a_{n,2} \ldots a_{n,n} \end{vmatrix};$$

во вторыхъ, если примѣнять ее надлежащимъ образомъ поочередно къ разнымъ сравненіямъ (1), то всегда можно дойти до такой *простѣйшей* системы:

$$(3)\quad \left\{\begin{array}{r} b_{1,1}x_1 + b_{1,2}x_2 + b_{1,3}x_3 + \ldots + b_{1,n}x_n + c_1 \equiv 0 \\ b_{2,2}x_2 + b_{2,3}x_3 + \ldots + b_{2,n}x_n + c_2 \equiv 0 \\ b_{3,3}x_3 + \ldots + b_{3,n}x_n + c_3 \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ b_{n,n}x_n + c_n \equiv 0 \end{array}\right\} \text{(mod. } k\text{)},$$

при чемъ будетъ имѣть мѣсто сравненіе

$$(4) \ldots\ldots\ldots b_{1,1}\, b_{2,2} \ldots b_{n,n} \equiv \pm \Delta \text{ (mod. } k\text{)}.$$

Рѣшеніе системы (1) приводится къ рѣшенію системы (3), а это послѣднее состоитъ очевидно въ послѣдовательномъ рѣшеніи n сравненій, каждое съ однимъ неизвѣстнымъ. Такимъ образомъ предложенная задача всегда приводится къ рѣшенію сравненія съ однимъ неизвѣстнымъ.

Если опредѣлитель Δ простой съ k, то каждый изъ коеффиціентовъ $b_{1,1}, b_{2,2}, \ldots b_{n,n}$ есть простой съ k; это видно изъ (4). Тогда каждое изъ сравненій (3), начиная съ послѣдняго, даетъ одно и только одно рѣшеніе для соотвѣтствующаго неизвѣстнаго, и поэтому система (1) имѣетъ одно и только одно рѣшеніе $(x_1, x_2, \ldots x_n)$. Напротивъ, если Δ не простое съ k, тогда по крайней мѣрѣ одинъ изъ коеффиціентовъ $b_{1,1}, b_{2,2}, \ldots b_{n,n}$, положимъ $b_{i,i}$, есть число не простое съ k, и потому сравненіе

$$b_{i,i}x_i + b_{i,i+1}x_{i+1} + \ldots + b_{i,n}x_n + c_i \equiv 0 \text{ (mod. } k\text{)},$$

помощью котораго опредѣляемъ x_i по извѣстнымъ ранѣе x_{i+1}, $x_{i+2}, \ldots x_n$, или не будетъ имѣть ни одного рѣшенія, или будетъ ихъ имѣть нѣсколько. Сообразно съ этимъ и система (1) или не будетъ имѣть вовсе рѣшеній, или будетъ ихъ имѣть нѣсколько.

На основаніи вышесказаннаго заключаемъ, что система однородныхъ линейныхъ сравненій

$$\left.\begin{array}{l} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n \equiv 0 \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,n}x_n \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,n}x_n \equiv 0 \end{array}\right\} (\text{mod. } k)$$

имѣетъ одно только очевидное рѣшеніе

$$x_1 \equiv x_2 \equiv x_3 \equiv \ldots \equiv x_n \equiv 0 \ (\text{mod. } k),$$

если ея опредѣлитель простой съ k; въ противномъ случаѣ она имѣетъ, кромѣ очевиднаго, еще одно или нѣсколько другихъ рѣшеній.

44. Понятно, что данную систему линейныхъ сравненій можно разными способами приводить къ простѣйшему виду; въ частныхъ случаяхъ могутъ встрѣчаться особенности, позволяющія быстро достигнуть цѣли, если ими воспользоваться удачно.

Случай, когда опредѣлитель системы и модуль взаимно простые. Примѣръ.

Въ случаѣ, если опредѣлитель системы простой съ модулемъ, нѣтъ надобности для опредѣленія рѣшеній приводить систему къ простѣйшему виду: можемъ написать прямо всѣ рѣшенія, пользуясь общеизвѣстными формулами изъ теоріи опредѣлителей.

Дѣйствительно, положимъ что дана система сравненій

$$(1) \ldots\ldots \left\{\begin{array}{l} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n \equiv b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,n}x_n \equiv b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,n}x_n \equiv b_n \end{array}\right\} (\text{mod. } k),$$

опредѣлитель которой обозначимъ чрезъ Δ. Изображая чрезъ Δ_i опредѣлитель составленный по формулѣ

$$\Delta_i = \begin{vmatrix} a_{1,1}\, a_{1,2} \ldots a_{1,i-1}\, b_1\, a_{1,i+1} \ldots a_{1,n} \\ a_{2,1}\, a_{2,2} \ldots a_{2,i-1}\, b_2\, a_{2,i+1} \ldots a_{2,n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}\, a_{n,2} \ldots a_{n,i-1}\, b_n\, a_{n,i+1} \ldots a_{n,n} \end{vmatrix},$$

при чемъ значекъ i принимаетъ всѣ значенія отъ 1 до n, для опредѣленія неизвѣстныхъ имѣемъ систему

$$(2) \ldots\ldots\ldots\ldots \left\{ \begin{array}{l} \Delta x_1 \equiv \Delta_1 \\ \Delta x_2 \equiv \Delta_2 \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ \Delta x_n \equiv \Delta_n \end{array} \right\} (\text{mod.}\, k),$$

равносильную съ (1).

Если опредѣлитель Δ не простой съ k, то относительно системы (2) можно сказать только то, что она есть слѣдствіе (1), но нельзя утверждать обратное, что (1) есть слѣдствіе (2).

Примѣръ. Найти всѣ рѣшенія трехъ сравненій

$$\left. \begin{array}{r} 2x - 3y + 5z \equiv 5 \\ 3x + 2y + 7z \equiv -1 \\ 5x - 4y + 6z \equiv 1 \end{array} \right\} (\text{mod. } 18).$$

Данная система равносильна слѣдующей:

$$\left. \begin{array}{r} 2x - 3y + 5z \equiv 5 \\ x + 5y + 2z \equiv -6 \\ x + 2y - 4z \equiv 9 \end{array} \right\} (\text{mod. } 18);$$

эта равносильна такой:

$$\left.\begin{aligned} x+2y-4z &\equiv 9 \\ 3y+6z &\equiv 3 \\ 7y+5z &\equiv -5 \end{aligned}\right\} \text{(mod. 18)}.$$

Беремъ теперь во вниманіе систему двухъ послѣднихъ сравненій

$$\left.\begin{aligned} 3y+6z &\equiv 3 \\ 7y+5z &\equiv -5 \end{aligned}\right\} \text{(mod. 18)}$$

и замѣчаемъ, что она равносильна слѣдующей:

$$\left.\begin{aligned} 3y+6z &\equiv 3 \\ y-7z &\equiv 7 \end{aligned}\right\} \text{(mod. 18)},$$

а эта въ свою очередь равносильна такой:

$$\left.\begin{aligned} y-7z &\equiv 7 \\ 9z &\equiv 0 \end{aligned}\right\} \text{(mod. 18)}.$$

На этомъ кончаются наши преобразованія, причемъ заключаемъ, что данная система сравненій приводится къ слѣдующему простѣйшему виду:

$$\left.\begin{aligned} x+2y-4z &\equiv 9 \\ y-7z &\equiv 7 \\ 9z &\equiv 0 \end{aligned}\right\} \text{(mod. 18)}.$$

Послѣднее сравненіе даетъ девять рѣшеній для z; для каждаго изъ нихъ два первыя сравненія даютъ по одному y и по одному x. Слѣдовательно число всѣхъ рѣшеній есть девять; вотъ они:

$$\left.\begin{array}{lrrrrrrrrr} x \equiv & -5, & -7, & -3, & 9, & -1, & 7, & 1, & 5, & 3 \\ y \equiv & 7, & 3, & -7, & -1, & -3, & -5, & 1, & 9, & 5 \\ z \equiv & 0, & 2, & -2, & 4, & -4, & 6, & -6, & 8, & -8 \end{array}\right\} \text{(mod. 18)}.$$

ГЛАВА IV.

Сравненія второй степени. — Законъ взаимности простыхъ чиселъ.

§ I. Приведеніе сравненія второй степени къ простѣйшему виду. Условіе рѣшимости въ случаѣ, когда модуль простой.

Простейшая форма сравнений второй степени.

45. Для сравненій степени выше первой особенную важность представляетъ случай, когда модуль простой. Тогда изысканія значительно облегчаются и получается возможность дѣлать общія заключенія. Поэтому-то здѣсь мы ограничимся сначала предположеніемъ, что модуль простой.

Если модуль равенъ 2, то для всякаго числа x имѣетъ мѣсто очевидное сравненіе

$$x^2 \equiv x \ (\text{mod. } 2),$$

вслѣдствіе чего сравненіе второй степени

$$ax^2 + bx + c \equiv 0 \ (\text{mod. } 2)$$

приводится къ сравненію первой степени

$$(a + b)x + c \equiv 0 \ (\text{mod. } 2).$$

Случай этотъ, какъ видимъ, не представляетъ ничего новаго; мы оставимъ его въ сторонѣ, и впредь будемъ постоянно подразумѣвать, что модуль $p > 2$.

Въ сравненіи второй степени

$$(1) \ldots\ldots\ldots ay^2 + by + c \equiv 0 \pmod{p}$$

коэффиціентъ a не долженъ дѣлиться на p: въ противномъ случаѣ сравненіе было бы первой степени. Если коэффиціентъ a не равенъ 1, то, найдя число a', удовлетворяющее условію

$$aa' \equiv 1 \pmod{p},$$

мы умножимъ обѣ части (1) на a'. Замѣняя послѣ этого произведеніе aa' его вычетомъ, равнымъ 1, получаемъ на мѣсто (1)

$$(2) \ldots\ldots\ldots y^2 + ly + m \equiv 0 \pmod{p},$$

гдѣ l и m изображаютъ вычеты чиселъ ba' и ca'.

Это первое упрощеніе сравненія второй степени.

Далѣе замѣчаемъ, что въ (2) коэффиціентъ l можно предположить четнымъ: ибо въ противномъ случаѣ стоитъ только на мѣсто l подставить $l - p$ или $l + p$; полагая слѣдовательно $l = 2d$, мы можемъ сравненіе (2) написать такъ:

$$(y + d)^2 \equiv d^2 - m \pmod{p},$$

или, называя для сокращенія

$$(3) \ldots\ldots\ldots y + d = x, \quad d^2 - m = q,$$

имѣемъ

$$(4) \ldots\ldots\ldots\ldots x^2 \equiv q \pmod{p}.$$

Это есть простѣйшая форма, подъ которой представляется всякое сравненіе второй степени.

Каждое рѣшеніе послѣдняго сравненія опредѣляетъ съ помощью (3) соотвѣтствующее рѣшеніе сравненія (1); если (4) невозможно, то и (1) также невозможно.

Если $q \equiv 0 \pmod{p}$, то (4) имѣетъ одно только рѣшеніе, именно $x \equiv 0 \pmod{p}$. Оставимъ этотъ случай въ сторонѣ, и будемъ впредь предполагать, что q не дѣлится на p.

Число рѣшеній.

46. **Теорема.** *Если q не дѣлится на p, то сравненіе*

(1) . . . . $x^2 \equiv q \pmod{p}$

или невозможно, или имѣетъ два рѣшенія.

Дѣйствительно, сравненіе (1) тогда только имѣетъ рѣшеніе, когда q сравнимо по модулю p по крайней мѣрѣ съ однимъ изъ чиселъ

$$1^2,\ 2^2,\ 3^2, \ldots (p-1)^2; \ ^{x)}$$

нуль пропущенъ здѣсь потому, что онъ не можетъ удовлетворять (1).

Такъ какъ члены равноудаленные отъ концовъ въ послѣднемъ ряду очевидно сравнимы между собой по модулю p, то слѣдовательно достаточно удержать половину всего ихъ числа, именно:

(2) . . . . $1^2,\ 2^2,\ 3^2, \ldots \left(\frac{p-1}{2}\right)^2.$

Всѣ числа въ (2) несравнимы по модулю p; ибо, допустивъ противное,

$$i^2 \equiv j^2 \pmod{p},$$

гдѣ $i < \frac{p}{2}$ и $j < \frac{p}{2}$, получаемъ

$$(i-j)(i+j) \equiv 0 \pmod{p},$$

что невозможно, такъ какъ числовая величина каждаго изъ множителей въ первой части меньше p.

Можно всегда предполагать, что въ (1) число q есть положительное и $< p$. Тогда, обозначая наименьшіе положительные вычеты чиселъ (2) соотвѣтственно чрезъ

(3) . . . . $r_1,\ r_2,\ r_3, \ldots r_{\frac{p-1}{2}},$

x) ибо $q \equiv x^2 \pmod{p}$; сравненіе же q со всякимъ инымъ числомъ $(p+i)^2$ приводится к сравненію q съ i^2, такъ такъ какъ $(p+i)^2 - i^2 = p^2+2pi \equiv 0 \pmod{p}$.

на основаніи вышесказаннаго заключаемъ, *что сравненіе* (1) *будетъ возможно или невозможно, смотря по тому будетъ ли число q содержаться въ ряду* (3), *или не будетъ.*

Допустивъ, что сравненіе (1) имѣетъ рѣшеніе $x=a$, мы замѣчаемъ, что и значеніе $x=-a$ будетъ также удовлетворять (1).

Числа a и $-a$ составляютъ различныя рѣшенія (1); ибо въ противномъ случаѣ должно было бы имѣть мѣсто сравненіе

$$a \equiv -a \pmod{p},$$

или

$$2a \equiv 0 \pmod{p},$$

что невозможно.

Другихъ рѣшеній, кромѣ двухъ означенныхъ, сравненіе (1) имѣть не можетъ; ибо изъ двухъ сравненій

$$x^2 \equiv q, \quad a^2 \equiv q \pmod{p},$$

выводимъ

$$x^2 - a^2 \equiv 0 \pmod{p},$$

или

$$(x-a)(x+a) \equiv 0 \pmod{p},$$

а это требуетъ, чтобы имѣло мѣсто одно изъ двухъ:

$$x \equiv a \pmod{p},$$

или

$$x \equiv -a \pmod{p}.$$

Такъ убѣждаемся въ справедливости предложенной теоремы.

47. **Теорема.** *Сравненіе $x^2 \equiv q \pmod{p}$ возможно или невозможно, смотря по тому имѣетъ ли мѣсто сравненіе* Условія возможности рѣшенія.

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

или не имѣетъ.

1. Необходимость означеннаго условія провѣряется очень легко съ помощью теоремы Фермата. Въ самомъ дѣлѣ, если существуетъ число x, удовлетворяющее сравненію

(1) . . . . $x^2 \equiv q \pmod{p}$,

то возвышая обѣ части въ степень $\frac{p-1}{2}$ и замѣчая, что по теоремѣ Фермата

$$x^{p-1} \equiv 1 \pmod{p},$$

получаемъ

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

2. Труднѣе доказать, что это условіе есть достаточное. Для этого можно воспользоваться тожествомъ (n^0 34)

$$(x-1^2)(x-2^2)\ldots\left(x-\left(\frac{p-1}{2}\right)^2\right) = x^{\frac{p-1}{2}} - 1 + pf(x).$$

Дѣлая въ немъ $x = q$, получаемъ

$$(q-1^2)(q-2^2)\ldots\left(q-\left(\frac{p-1}{2}\right)^2\right) = q^{\frac{p-1}{2}} - 1 + pf(q);$$

а такъ какъ значеніе $f(q)$ есть цѣлое, то можно слѣдовательно написать

(2) $(q-1^2)(q-2^2)\ldots\left(q-\left(\frac{p-1}{2}\right)^2\right) \equiv q^{\frac{p-1}{2}} - 1 \pmod{p}$.

Если сравненіе (1) возможно, то q сравнимо съ однимъ изъ чиселъ $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$, ($n^0$ 46); поэтому одинъ изъ множителей въ первой части сравненія (2) дѣлится на p, и слѣдовательно имѣемъ

(3) . . . . $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Наоборотъ, если условіе (3) удовлетворено, то (2) принимаетъ видъ

$$(q-1^2)(q-2^2)\ldots\left(q-\left(\frac{p-1}{2}\right)^2\right) \equiv 0 \pmod{p};$$

отсюда видно, что q сравнимо съ однимъ изъ чиселъ $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$ и поэтому сравненіе (1) имѣетъ рѣшеніе. Справедливость теоремы такимъ образомъ доказана.

Слѣдствіе. *Сравненіе* $x^2 \equiv q \pmod{p}$ *возможно или невозможно, смотря по тому будетъ ли значеніе символа* $\left(\frac{q}{p}\right)$ *равняться* $+1$ *или* -1.

Это вытекаетъ прямо изъ опредѣленія символа Лежандра, даннаго нами въ n^0 33. стр. 82.

§ II. Символъ Лежандра, его свойства. Законъ взаимности простыхъ чиселъ.

48. Все, что до сихъ поръ было нами высказано о символѣ Лежандра,*) заключается въ слѣдующихъ трехъ предложеніяхъ. Основныя свойства символа Лежандра.

1°. Числовая величина символа $\left(\frac{q}{p}\right)$ всегда равна 1.

2°. Символъ $\left(\frac{q}{p}\right)$ опредѣляется сравненіемъ

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}.$$

3°. Чтобы сравненіе $x^2 \equiv q \pmod{p}$ было возможно, необходимо и достаточно условіе

$$\left(\frac{q}{p}\right) = 1.$$

Послѣднее предложеніе заставляетъ обратить особенное вниманіе на символъ Лежандра и войти въ подробное изученіе его свойствъ. Изслѣдованія этого рода привели къ результатамъ въ высшей степени самимъ по себѣ замѣчательнымъ и въ то же время весьма важнымъ для дальнѣйшихъ изысканій въ теоріи чиселъ.

Теорема 1. *Величина символа* $\left(\frac{1}{p}\right)$ *есть* 1, *а символа* $\left(\frac{-1}{p}\right)$ *есть* $(-1)^{\frac{p-1}{2}}$.

*) n. 33 стр. 82. Если a не дѣлится на p, гдѣ p число простое и не равное 2, то $a^{\frac{p-1}{2}} \equiv +1 \pmod{p}$ или $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Символъ Лежандра $\left(\frac{a}{p}\right)$ есть то изъ двухъ чиселъ $+1$ или -1, съ которымъ сравнимо число $a^{\frac{p-1}{2}}$ по модулю p.

Дѣйствительно, если въ сравненіи

$$\left(\frac{q}{p}\right) - q^{\frac{p-1}{2}} \equiv 0 \ (\text{mod.}\, p)$$

сдѣлаемъ $q = \pm 1$, то числовое значеніе первой части не будетъ превышать 2, между тѣмъ модуль p предполагается болѣе 2; слѣдовательно

$$\left(\frac{q}{p}\right) - q^{\frac{p-1}{2}} = 0, \quad (q = \pm 1),$$

то есть

$$\left(\frac{1}{p}\right) = 1,$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

что и слѣдовало доказать.

Слѣдствіе. *Сравненіе* $x^2 + 1 \equiv 0$ (mod. p) *возможно въ томъ только случаѣ, когда простое число* p *есть вида* $4n + 1$.

Дѣйствительно, всякое нечетное простое число есть вида $4n + 1$ или $4n + 3$. Въ первомъ случаѣ имѣемъ

$$\left(\frac{-1}{p}\right) = (-1)^{2n} = 1;$$

во второмъ

$$\left(\frac{-1}{p}\right) = (-1)^{2n+1} = -1.$$

Слѣдовательно въ первомъ случаѣ сравненіе $x^2 + 1 \equiv 0$ (mod. p) возможно, во второмъ невозможно. Когда оно возможно, рѣшеніе опредѣляется по теоремѣ Вильсона, именно стр. 90.

$$x \equiv \pm 1.\ 2.\ 3 \ldots \frac{p-1}{2} \ (\text{mod.}\, p).$$

Теорема 2. *Если* q *есть произведеніе чиселъ* $q_1, q_2, \ldots q_m$, *то*

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots \left(\frac{q_m}{p}\right).$$

Дѣйствительно, перемножая почленно сравненія

$$q_1^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) (\mathrm{mod.}\, p),$$

$$q_2^{\frac{p-1}{2}} \equiv \left(\frac{q_2}{p}\right) (\mathrm{mod.}\, p),$$

. . . .

. . . .

$$q_m^{\frac{p-1}{2}} \equiv \left(\frac{q_m}{p}\right) (\mathrm{mod.}\, p),$$

получаемъ

$$(q_1\, q_2 \ldots q_m)^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots \left(\frac{q_m}{p}\right) (\mathrm{mod.}\, p).$$

Но

$$(q_1\, q_2 \ldots q_m)^{\frac{p-1}{2}} = q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) (\mathrm{mod.}\, p);$$

слѣдовательно

$$\left(\frac{q}{p}\right) \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots \left(\frac{q_m}{p}\right) (\mathrm{mod.}\, p).$$

Числовая величина какъ первой такъ и второй части послѣдняго сравненія равна 1; поэтому, еслибы эти части не были равны между собой, мы имѣли бы сравненіе

$$1 \equiv -1 \ (\mathrm{mod.}\, p),$$

или

$$2 \equiv 0 \ (\mathrm{mod.}\, p),$$

что невозможно при $p > 2$. Итакъ, предыдущее сравненіе приводитъ къ уравненію

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots \left(\frac{q_m}{p}\right),$$

что и слѣдовало доказать.

Слѣдствіе 1. *Символъ* $\left(\frac{q^n}{p}\right)$ *равенъ величинѣ символа* $\left(\frac{q}{p}\right)$, *возведенной въ степень* n.

Слѣдствіе 2. *При опредѣленіи величины символа* $\left(\frac{q}{p}\right)$ *мы можемъ исключать изъ* q *всякій множитель, составляющій точный квадратъ.*

Дѣйствительно, по доказанной теоремѣ мы имѣемъ

$$\left(\frac{q_1 q_2^2}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2^2}{p}\right);$$

но

$$\left(\frac{q_2^2}{p}\right) = \left(\frac{q_2}{p}\right)^2 = (\pm 1)^2 = 1,$$

слѣдовательно

$$\left(\frac{q_1 q_2^2}{p}\right) = \left(\frac{q_1}{p}\right).$$

Теорема 3. *Если* q *и* q_1 *сравнимы по модулю* p, *то*

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right).$$

Въ самомъ дѣлѣ, возвышая обѣ части сравненія

$$q \equiv q_1 \pmod{p}$$

въ степень $\frac{p-1}{2}$, получаемъ

$$q^{\frac{p-1}{2}} \equiv q_1^{\frac{p-1}{2}} \pmod{p};$$

отсюда же заключаемъ

$$\left(\frac{q}{p}\right) \equiv \left(\frac{q_1}{p}\right) \pmod{p}.$$

Сравненіе это показываетъ невозможность уравненія $\left(\frac{q}{p}\right) = -\left(\frac{q_1}{p}\right)$; ибо тогда мы имѣли бы

$$\left(\frac{q}{p}\right) \equiv -\left(\frac{q}{p}\right) \pmod{p},$$

или

$$2\left(\frac{q}{p}\right) \equiv 0 \pmod{p},$$

что очевидно не имѣетъ мѣста при $p > 2$. Слѣдовательно

$$\left(\frac{q}{p}\right)=\left(\frac{q_1}{p}\right),$$

что и требовалось доказать.

Теорема 4. *Если обозначимъ чрезъ m число чиселъ въ ряду*

$$q,\ 2q,\ 3q,\ldots\frac{p-1}{2}q,$$

коихъ абсолютно-малые вычеты по модулю p отрицательны, то

$$\left(\frac{q}{p}\right)=(-1)^m.$$

Замѣтимъ прежде всего, что такъ какъ q предполагается не дѣлящимся на p, то каждое изъ чиселъ, содержащихся въ означенномъ ряду, очевидно не дѣлится на p и слѣдовательно знакъ его абсолютно малаго вычета по модулю p вполнѣ опредѣленъ. Принимая это къ свѣдѣнію, обозначимъ абсолютно малый вычетъ произведенія iq чрезъ $(-1)^{e_i} r_i$, причемъ r_i есть числовая величина вычета, а e_i равно нулю или 1, смотря по тому будетъ ли этотъ вычетъ положительнымъ или отрицательнымъ. Имѣемъ рядъ сравненій

$$\left.\begin{array}{r}
q\equiv(-1)^{e_1}r_1\\
2q\equiv(-1)^{e_2}r_2\\
3q\equiv(-1)^{e_3}r_3\\
\ldots\ldots\ldots\ldots\\
\ldots\ldots\ldots\ldots\\
\frac{p-1}{2}q\equiv(-1)^{e_{\frac{p-1}{2}}}r_{\frac{p-1}{2}}
\end{array}\right\}\ (\mathrm{mod.}\,p),$$

которыя перемножая почленно, получаемъ

$$(1)\ldots 1.\,2.\,3\ldots\frac{p-1}{2}\,q^{\frac{p-1}{2}}\equiv(-1)^{e_1+e_2+\ldots+e_{\frac{p-1}{2}}}$$

$$\times\, r_1\, r_2\ldots r_{\frac{p-1}{2}}\ (\mathrm{mod.}\,p).$$

Числа $r_1, r_2, \ldots r_{\frac{p-1}{2}}$ содержатся въ ряду

$$1, 2, 3, \ldots \frac{p-1}{2}$$

и всѣ различны; ибо допустивъ $r_i = r_j$, получаемъ отсюда сравненіе

$$(-1)^{e_i} iq \equiv (-1)^{e_j} jq \pmod{p},$$

что по сокращеніи на q можно написать такъ:

$$i - (-1)^{e_i + e_j} j \equiv 0 \pmod{p},$$

а это невозможно потому, что числовая величина первой части менѣе p и не равна нулю.

Итакъ, числа $r_1, r_2, \ldots r_{\frac{p-1}{2}}$ составляютъ нѣкоторую перестановку чиселъ $1, 2, \ldots \frac{p-1}{2}$; слѣдовательно

$$1.\ 2.\ 3 \ldots \frac{p-1}{2} = r_1 r_2 \ldots r_{\frac{p-1}{2}}.$$

Замѣчая теперь, что произведеніе $1.\ 2 \ldots \frac{p-1}{2}$ не дѣлится на p, мы можемъ сократить обѣ части (1) на равные множители и написать

$$q^{\frac{p-1}{2}} \equiv (-1)^{e_1 + e_2 + \ldots + e_{\frac{p-1}{2}}} \pmod{p}.$$

Изъ опредѣленія чиселъ $e_1, e_2, \ldots$ слѣдуетъ, что сумма $e_1 + e_2 + \ldots + e_{\frac{p-1}{2}}$ равна m; сверхъ того имѣемъ

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p};$$

слѣдовательно предыдущее сравненіе приводитъ къ такому:

$$\left(\frac{q}{p}\right) \equiv (-1)^m \pmod{p}.$$

Отсюда заключаемъ, что $\left(\frac{q}{p}\right) = (-1)^m$, что и требовалось доказать.

Теорема 5. *Величина символа* $\left(\frac{2}{p}\right)$ *есть* $(-1)^{\frac{p^2-1}{8}}$.

Основываясь на предшествующей теоремѣ, мы заключаемъ, что величина символа $\left(\frac{2}{p}\right)$ равняется числу чиселъ въ ряду

$$2,\ 4,\ 6,\ 8, \ldots p-1,$$

коихъ абсолютно малые вычеты отрицательны или, другими словами, коихъ наименьшіе положительные вычеты болѣе $\frac{p}{2}$. Принимая это во вниманіе, мы разсмотримъ отдѣльно два случая:

Первый случай, p есть вида $4n+1$. Тогда имѣемъ $p-1 = 4n$, $\frac{p}{2} = 2n + \frac{1}{2}$, и приходится сосчитать, сколько въ ряду

$$2,\ 4,\ 6,\ 8, \ldots 4n$$

содержится чиселъ, превышающихъ $2n+\frac{1}{2}$. Эти числа суть слѣдующія:

$$2n+2,\ 2n+4,\ 2n+6, \ldots 4n;$$

число ихъ равно n; поэтому имѣемъ

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p-1}{4}}.$$

Съ другой стороны, на основаніи равенства

$$\frac{(p^2-1)}{8} = \frac{p-1}{4} + 2n^2,$$

заключаемъ о справедливости уравненія

$$(-1)^{\frac{p-1}{4}} = (-1)^{\frac{p^2-1}{8}},$$

вслѣдствіе чего предыдущую формулу для $\left(\frac{2}{p}\right)$ можно написать такъ:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Это показываетъ справедливость предложенной теоремы въ разсматриваемомъ частномъ случаѣ.

Второй случай, p есть вида $4n+3$. Имѣемъ $p-1=4n+2$, $\frac{p}{2}=2n+1+\frac{1}{2}$. Числа, содержащіяся въ ряду

$$2,\ 4,\ 6,\ldots 4n+2$$

и превышающія $2n+1+\frac{1}{2}$, суть слѣдующія:

$$2n+2,\ 2n+4,\ 2n+6,\ldots 4n+2.$$

Число ихъ равно $n+1$; слѣдовательно

$$\left(\frac{2}{p}\right)=(-1)^{n+1}=(-1)^{\frac{p+1}{4}}.$$

Замѣчая теперь, что

$$\frac{p^2-1}{8}=\frac{p+1}{4}+2n(n+1),$$

имѣемъ

$$(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p+1}{4}},$$

откуда заключаемъ

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Этимъ теорема доказана вполнѣ.

Слѣдствіе. *Если простое число p есть вида* $8n\pm 1$, *то* $\left(\frac{2}{p}\right)=1$; *если же оно есть вида* $8n\pm 3$, *то* $\left(\frac{2}{p}\right)=-1$.

Дѣйствительно, въ первомъ случаѣ имѣемъ

$$\frac{p^2-1}{8}=\frac{64n^2\pm 16n}{8}=2n(4n\pm 1),$$

во второмъ

$$\frac{p^2-1}{8}=\frac{64n^2\pm 48n+8}{8}=2n(4n\pm 3)+1;$$

слѣдовательно въ первомъ случаѣ $\frac{p^2-1}{8}$ есть число четное, во второмъ нечетное, и сообразно съ этимъ имѣемъ $\left(\frac{2}{p}\right)=1$ или $\left(\frac{2}{p}\right)=-1$.

49. Основываясь на предыдущихъ теоремахъ, мы заключаемъ, что опредѣленіе всякаго символа $\left(\frac{q}{p}\right)$ можно свести на вычисленіе одного или нѣсколькихъ символовъ $\left(\frac{r}{p}\right), \left(\frac{r'}{p}\right), \ldots$, въ которыхъ члены $r, r', \ldots$ будутъ положительными, нечетными и менѣе $\frac{p}{2}$.

Возьмемъ для примѣра символъ $\left(\frac{956}{613}\right)$. Наименьшій отрицательный вычетъ числа 956 по модулю 613 есть -270; поэтому имѣемъ

$$\left(\frac{956}{613}\right)=\left(\frac{-270}{613}\right)=\left(\frac{-1}{613}\right)\left(\frac{270}{613}\right)=\left(\frac{270}{613}\right).$$

Разлагая 270 на простые множители, находимъ $270 = 2 \cdot 3^3 \cdot 5$; слѣдовательно

$$\left(\frac{270}{613}\right)=\left(\frac{2}{613}\right)\left(\frac{3}{613}\right)\left(\frac{5}{613}\right).$$

Такъ какъ число 613 есть вида $8n-3$, то $\left(\frac{2}{613}\right)=-1$; вслѣдствіе этого можно написать

$$\left(\frac{956}{613}\right)=-\left(\frac{3}{613}\right)\left(\frac{5}{613}\right).$$

Вычисленіе заданнаго символа приводится такимъ образомъ къ вычисленію двухъ другихъ символовъ, въ которыхъ верхніе члены суть 3 и 5.

Тѣ же самыя теоремы даютъ иногда возможность опредѣлить значеніе даннаго символа.

Напримѣръ, для $p=31$, находимъ

$$\left(\frac{3}{31}\right)=\left(\frac{27}{31}\right)=\left(\frac{27-31}{31}\right)=\left(\frac{-4}{31}\right)=\left(\frac{-1}{31}\right)=-1,$$

$$\left(\frac{5}{31}\right)=\left(\frac{5-31}{31}\right)=\left(\frac{-26}{31}\right)=-\left(\frac{2}{31}\right)\left(\frac{13}{31}\right)=-\left(\frac{13}{31}\right)$$

$$=-\left(\frac{13-31}{31}\right)=-\left(\frac{-18}{31}\right)=\left(\frac{2}{31}\right)=1,$$

$$\left(\frac{7}{31}\right)=\left(\frac{7-31}{31}\right)=\left(\frac{-24}{31}\right)=-\left(\frac{2}{31}\right)\left(\frac{3}{31}\right)=1,$$

$$\left(\frac{11}{31}\right)=\left(\frac{-20}{31}\right)=-\left(\frac{5}{31}\right)=-1,$$

$$\left(\frac{13}{31}\right)=\left(\frac{-18}{31}\right)=-\left(\frac{2}{31}\right)=-1,$$

$$\left(\frac{15}{31}\right)=\left(\frac{-16}{31}\right)=-1.$$

Доказательство закона взаимности.

50. Пусть p и q изображаютъ два какія нибудь различныя простыя числа, оба болѣе 2. Всякое число a, не дѣлящееся на произведеніе pq, даетъ относительно модулей p и q два соотвѣтствующихъ, абсолютно малыхъ вычета, знаки которыхъ суть опредѣленные, за исключеніемъ одного случая, когда a дѣлится на p или на q; тогда одинъ изъ означенныхъ абсолютно малыхъ вычетовъ будетъ равенъ нулю, вслѣдствіе чего знакъ его будетъ неопредѣленнымъ.

Сообразно этому всѣ числа не дѣлящіяся на pq можно распредѣлить на восемь классовъ въ порядкѣ указанномъ слѣдующею таблицей:

Абсолютно малый вычетъ	по модулю p	0	0	+	—	+	—	+	—
	по модулю q	+	—	0	0	+	—	—	+
Классъ		I	II	III	IV	V	VI	VII	VIII

Очевидно, что числа, сравнимыя по модулю pq, принадлежатъ къ одному и тому же классу, и если согласимся такія числа не считать за различныя, то можно будетъ сказать, что число чиселъ, принадлежащихъ къ какому нибудь изъ вышеперечисленныхъ классовъ, опредѣляется числомъ чиселъ, содержащихся въ ряду

(1) . . . . 1, 2, 3, 4, . . . $pq-1$

и принадлежащихъ къ этому классу.

Такъ какъ числа p и q взаимно простыя, то, каковы бы ни были числа a и b, всегда въ (1) найдется одно и только одно число x, удовлетворяющее одновременно двумъ условіямъ

$$x \equiv a \ (\text{mod.}\, p), \quad x \equiv b \ (\text{mod.}\, q).$$

Это даетъ возможность опредѣлить число чиселъ, принадлежащихъ къ каждому классу. Обозначивъ чрезъ n_i число чиселъ, принадлежащихъ къ i-ому классу, имѣемъ

$$(2) \ldots\ldots \begin{cases} n_1 = n_2 = \frac{q-1}{2}, \quad n_3 = n_4 = \frac{p-1}{2}, \\ n_5 = n_6 = n_7 = n_8 = \frac{(p-1)(q-1)}{4}, \end{cases}$$

при чемъ

$$n_1 + n_2 + \ldots + n_8 = pq - 1.$$

Раздѣливъ теперь числа (1) на двѣ отдѣльныя группы

$$(3) \ldots\ldots\ldots\ldots 1, 2, 3, \ldots \frac{pq-1}{2},$$

$$(4) \ldots\ldots\ldots\ldots \frac{pq+1}{2}, \frac{pq+3}{2}, \ldots pq-1,$$

изъ коихъ первая состоитъ изъ чиселъ $< \frac{pq}{2}$, а вторая изъ чиселъ $> \frac{pq}{2}$, мы обозначимъ соотвѣтственно чрезъ v_i и v'_i число чиселъ въ (3) и (4), принадлежащихъ къ i-ому классу. Получаемъ такимъ образомъ 16 новыхъ чиселъ $v_1, v_2, \ldots v_8$, $v'_1, v'_2, \ldots v'_8$, между которыми имѣютъ мѣсто нѣсколько очень простыхъ зависимостей. Прежде всего укажемъ на тѣ соотношенія между числами v_i и v'_i, которыя вытекаютъ почти непосредственно изъ самаго ихъ опредѣленія. Во первыхъ, очевидно, что $v_i + v'_i = n_i$. Это даетъ такую группу уравненій:

$$(5) \begin{cases} v_1 + v'_1 = v_2 + v'_2 = \frac{q-1}{2}, \quad v_3 + v'_3 = v_4 + v'_4 = \frac{p-1}{2}, \\ v_5 + v'_5 = v_6 + v'_6 = v_7 + v'_7 = v_8 + v'_8 = \frac{(p-1)(q-1)}{4}. \end{cases}$$

Далѣе мы замѣчаемъ, что если число a содержится въ (3) и принадлежитъ къ первому классу, то $pq - a$ содержится въ (4) и принадлежитъ ко второму классу. Равнымъ образомъ и наоборотъ, всякому числу a въ (4), принадлежащему ко второму классу, соотвѣтствуетъ въ (3) число $pq - a$, принадлежащее къ первому классу. Поэтому ясно, что $v_1 = v'_2$.

Разсуждая подобно предыдущему, можно убѣдиться въ справедливости всѣхъ нижеслѣдующихъ равенствъ:

$$(6)\ldots\left\{\begin{array}{llll} v_1 = v'_2, & v_3 = v'_4, & v_5 = v'_6, & v_7 = v'_8, \\ v'_1 = v_2, & v'_3 = v_4, & v'_5 = v_6, & v'_7 = v_8, \end{array}\right.$$

на основаніи которыхъ, задача о вычисленіи 16 чиселъ v_i, v'_i приводится къ опредѣленію половины всего ихъ числа, именно: $v_1, v_2, \ldots v_8$.

Изъ (5) и (6) выводимъ

$$(7)\ldots\ldots\left\{\begin{array}{l} v_1 + v_2 = \frac{q-1}{2}, \quad v_3 + v_4 = \frac{p-1}{2}, \\ v_5 + v_6 = v_7 + v_8 = \frac{(p-1)(q-1)}{4}. \end{array}\right.$$

Чтобы получить еще другія соотношенія между числами $v_1, \ldots v_8$, мы предлагаемъ себѣ вопросъ: каково число чиселъ въ (3), коихъ абсолютно малые вычеты по модулю q отрицательны.

Очевидно, что это число равно суммѣ $v_2 + v_6 + v_7$; но, съ другой стороны, числа, о которыхъ идетъ рѣчь, суть слѣдующія:

$$\frac{q+1}{2},\ \frac{q+3}{2},\ \frac{q+5}{2}, \ldots q-1,$$

$$q + \frac{q+1}{2},\ q + \frac{q+3}{2},\ q + \frac{q+5}{2}, \ldots 2q-1,$$

$$2q + \frac{q+1}{2},\ 2q + \frac{q+3}{2},\ 2q + \frac{q+5}{2}, \ldots 3q-1,$$

. . . .

. . . .

$$\frac{p-3}{2}q + \frac{q+1}{2},\ \frac{p-3}{2}q + \frac{q+3}{2},\ \frac{p-3}{2}q + \frac{q+5}{2} \ldots \frac{p-3}{2}q + q - 1.$$

Отсюда видно непосредственно, что ихъ число равно $\frac{(p-1)(q-1)}{4}$; слѣдовательно

$$(8) \ldots\ldots\ldots v_2 + v_6 + v_7 = \frac{(p-1)(q-1)}{4}.$$

Подобнымъ образомъ удостовѣряемся въ справедливости формулы

$$(9) \ldots\ldots\ldots v_4 + v_6 + v_8 = \frac{(p-1)(q-1)}{4}.$$

Уравненія (7), (8), (9) не даютъ еще возможности выразить числа $v_1, v_2, \ldots v_8$, какъ функціи отъ p и q; для этого недостаётъ двухъ соотношеній, которыя должны принадлежать къ совершенно другому типу, чѣмъ предыдущія. Тѣмъ не менѣе изъ полученныхъ равенствъ вытекаетъ слѣдствіе, имѣющее очень большое значеніе въ теоріи чиселъ; оно и составляетъ главную цѣль настоящаго изысканія.

Замѣчая, что числа, содержащіяся въ (3) и принадлежащія къ четвертому классу, совпадаютъ съ тѣми числами въ ряду

$$q,\ 2q,\ 3q, \ldots \frac{p-1}{2}q,$$

коихъ абсолютно малые вычеты по модулю p отрицательны, мы заключаемъ на основаніи 4-ой теоремы предшествующаго номера о справедливости такого равенства

$$(10) \ldots\ldots\ldots\ldots \left(\frac{q}{p}\right) = (-1)^{v_4}.$$

Подобно этому имѣемъ также

$$(11) \ldots\ldots\ldots\ldots \left(\frac{p}{q}\right) = (-1)^{v_2}.$$

Съ другой стороны, изъ (8) и (9) выводимъ

$$v_2 + v_4 = \frac{(p-1)(q-1)}{2} - 2v_6 - (v_7 + v_8);$$

отсюда, внося на мѣсто $v_7 + v_8$ значеніе, опредѣляемое однимъ изъ (7), получаемъ

$$v_2 + v_4 = \frac{p-1}{2}\,\frac{q-1}{2} - 2v_6.$$

Слѣдовательно

$$(-1)^{v_2}(-1)^{v_4} = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

Внося въ первую часть послѣдняго равенства на мѣсто каждаго множителя соотвѣтствующее выраженіе по (10) и (11), получаемъ

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

Умножая обѣ части на $\left(\frac{q}{p}\right)$ и замѣчая, что $\left(\frac{q}{p}\right)^2 = 1$, предыдущую формулу можемъ написать такъ:

$$(12) \quad \ldots\ldots\ldots \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

Это и есть та формула, которую мы желали вывести. Она даетъ слѣдующую теорему.

Теорема. *Если p и q суть различныя простыя числа, оба болѣе 2, то*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

Слѣдствіе. *Если по крайней мѣрѣ одно изъ чиселъ p, q есть вида $4n + 1$, то*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right);$$

если же оба числа p и q суть вида $4n + 3$, то

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Эта зависимость между двумя взаимно обратными символами извѣстна подъ названіемъ закона взаимности простыхъ чиселъ. Гауссъ первый далъ строгое его доказательство; онъ далъ ихъ нѣсколько; то, которое мы изложили здѣсь, есть пятое.

51. Извѣстно, что знакъ абсолютно малаго вычета числа q по модулю p опредѣляется формулой

Доказате[…] закона вза[…] ности (про[…] жение).

$$(-1)^{E\frac{2q}{p}},$$

при чемъ $E\frac{2q}{p}$ изображаетъ наибольшее цѣлое число, заключающееся въ $\frac{2q}{p}$ (см. n^0 28). Это позволяетъ представить величину символа $\left(\frac{q}{p}\right)$ въ особенномъ видѣ.

Теорема 1. *Значеніе символа* $\left(\frac{q}{p}\right)$ *опредѣляется уравненіемъ*

$$\left(\frac{q}{p}\right)=(-1)^{E\frac{2q}{p}+E\frac{4q}{p}+\ldots+E\frac{(p-1)q}{p}}.$$

На самомъ дѣлѣ, обозначая знаки абсолютно малыхъ вычетовъ чиселъ

$$q,\ 2q,\ 3q,\ldots\frac{p-1}{2}q$$

соотвѣтственно чрезъ

$$(-1)^{e_1},\ (-1)^{e_2},\ (-1)^{e_3},\ldots(-1)^{e_{\frac{p-1}{2}}},$$

по одной изъ вышедоказанныхъ теоремъ имѣемъ

$$\left(\frac{q}{p}\right)=(-1)^{e_1+e_2+\ldots+e_{\frac{p-1}{2}}}.$$

Съ другой стороны, имѣемъ

$$(-1)^{e_1}=(-1)^{E\frac{2q}{p}},\ (-1)^{e_2}=(-1)^{E\frac{4q}{p}},\ (-1)^{e_3}=(-1)^{E\frac{6q}{p}},\ldots$$

$$(-1)^{e_{\frac{p-1}{2}}}=(-1)^{E\frac{(p-1)q}{p}};$$

слѣдовательно

$$(1)\ \ldots\ldots\left(\frac{q}{p}\right)=(-1)^{E\frac{2q}{p}+E\frac{4q}{p}+\ldots+E\frac{(p-1)q}{p}},$$

что и требовалось доказать.

Послѣдняя теорема справедлива при всякомъ числѣ q. Но не трудно вывести изъ нея, какъ слѣдствіе, другую, болѣе простую теорему, которая можетъ служить для опредѣленія $\left(\frac{q}{p}\right)$ при q нечетномъ.

Теорема 2. *Если число q нечетное, то значеніе $\left(\frac{q}{p}\right)$ опредѣляется уравненіемъ*

$$\left(\frac{q}{p}\right)=(-1)^{E\frac{q}{p}+E\frac{2q}{p}+\ldots+E\frac{\frac{1}{2}(p-1)q}{p}}.$$

Дѣйствительно, если q означаетъ какое нибудь нечетное число, не дѣлящееся на p, то сумма $q+p$ представляетъ число четное, не дѣлящееся на p, вслѣдствіе чего $\frac{1}{2}(q+p)$ представляетъ цѣлое число, не дѣлящееся на p. Принимая это во вниманіе, внесемъ въ обѣ части (1) $\frac{1}{2}(q+p)$ на мѣсто q; получаемъ

$$\left(\frac{\frac{1}{2}(q+p)}{p}\right)=(-1)^{E\frac{q+p}{p}+E\frac{2q+2p}{p}+\ldots+E\frac{\frac{p-1}{2}q+\frac{p-1}{2}p}{p}}.$$

Но

$$E\frac{q+p}{p}=1+E\frac{q}{p},$$

$$E\frac{2q+2p}{p}=2+E\frac{2q}{p},$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$E\frac{\frac{p-1}{2}q+\frac{p-1}{2}p}{p}=\frac{p-1}{2}+E\frac{\frac{p-1}{2}q}{p};$$

слѣдовательно

$$\left(\frac{\frac{1}{2}(q+p)}{p}\right)=(-1)^{1+2+\ldots+\frac{p-1}{2}+E\frac{q}{p}+E\frac{2q}{p}+\ldots+E\frac{\frac{p-1}{2}q}{p}},$$

или, проще,

$$\left(\frac{\frac{1}{2}(q+p)}{p}\right)=(-1)^{\frac{p^2-1}{8}+E\frac{q}{p}+E\frac{2q}{p}+\ldots+E\frac{\frac{p-1}{2}q}{p}}.$$

Умноживъ обѣ части этого уравненія на $\left(\frac{2}{p}\right)$, получаемъ

$$\left(\frac{2}{p}\right)\left(\frac{\frac{1}{2}(q+p)}{p}\right)=\left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}+E\frac{q}{p}+E\frac{2q}{p}+\ldots+E\frac{\frac{p-1}{2}q}{p}}.$$

Но по извѣстнымъ намъ теоремамъ имѣемъ

$$\left(\frac{2}{p}\right)\left(\frac{\frac{1}{2}(q+p)}{p}\right)=\left(\frac{q+p}{p}\right)=\left(\frac{q}{p}\right);$$

поэтому предыдущее уравненіе можно представить такъ:

$$(2)\ldots\left(\frac{q}{p}\right)=\left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}+E\frac{q}{p}+E\frac{2q}{p}+\ldots+E\frac{\frac{p-1}{2}q}{p}}.$$

Дѣлая здѣсь $q=1$ и замѣчая, что

$$\left(\frac{1}{p}\right)=1,\quad E\frac{1}{p}=E\frac{2}{p}=\ldots=E\frac{\frac{p-1}{2}}{p}=0,$$

находимъ

$$1=\left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}},$$

откуда выводимъ

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Этотъ результатъ представляетъ собой теорему 5-ую n^0 48, которая такимъ образомъ доказана нами вновь.

Внеся въ (2) величину $\left(\frac{2}{p}\right)$, находимъ

$$(3)\ldots\ldots\left(\frac{q}{p}\right)=(-1)^{E\frac{q}{p}+E\frac{2q}{p}+\ldots+E\frac{\frac{p-1}{2}q}{p}},$$

что и слѣдовало доказать.

Теорема 3. *Если q число нечетное и меньше p, то значеніе $\left(\frac{q}{p}\right)$ опредѣляется уравненіемъ*

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}-E\frac{p}{q}-E\frac{2p}{q}-\ldots-E\frac{\frac{q-1}{2}p}{q}}.$$

Для доказательства воспользуемся формулою, выражающей равенство цѣлой части количества x и числа цѣлыхъ чиселъ не превышающихъ x (см. n^0 9),

$$(4) \ldots\ldots\ Ex = e(x) + e\left(\frac{x}{2}\right) + e\left(\frac{x}{3}\right) + \ldots,$$

при чемъ знакъ $e(\omega)$ изображаетъ нуль или 1, смотря по тому, будетъ ли количество ω правильной дробью или неправильной.

Обозначая для сокращенія показатель во второй части (3) чрезъ M, и внося на мѣсто каждаго члена въ его выраженіи соотвѣтствующее значеніе по формулѣ (4), получаемъ

$$(5) \ldots\ldots\ldots\ldots \left(\frac{q}{p}\right) = (-1)^M$$

$$(6)\quad M = e\left(\frac{q}{p}\right) + e\left(\frac{q}{2p}\right) + \ldots + e\left(\frac{q}{np}\right) + \ldots$$
$$+ e\left(\frac{2q}{p}\right) + e\left(\frac{2q}{2p}\right) + \ldots + e\left(\frac{2q}{np}\right) + \ldots$$
$$+ e\left(\frac{3q}{p}\right) + e\left(\frac{3q}{2p}\right) + \ldots + e\left(\frac{3q}{np}\right) + \ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ e\left(\frac{\frac{p-1}{2}q}{p}\right) + e\left(\frac{\frac{p-1}{2}q}{2p}\right) + \ldots + e\left(\frac{\frac{p-1}{2}q}{np}\right) + \ldots$$

Во всякомъ столбцѣ второй части послѣдняго уравненія члены очевидно не могутъ убывать; поэтому если послѣдній изъ нихъ равенъ нулю, то и всѣ предшествующіе также равны нулю, и весь столбецъ будетъ состоять изъ однихъ нулей. За такимъ столбцомъ всѣ послѣдующіе столбцы будутъ очевидно также состоять изъ однихъ нулей. Отсюда слѣдуетъ, что въ формулѣ (6) можно удержать только тѣ столбцы, въ которыхъ послѣдніе элементы не равны нулю, всѣ же остальные отбросить. Но посмо-

тримъ, сколько въ послѣдней строкѣ (6) находится членовъ равныхъ 1. Чтобы n-ый членъ былъ равенъ 1, имѣемъ условіе

$$\frac{p-1}{2}q \geqq np,$$

откуда выводимъ

$$n \leqq \frac{q-1}{2} + \frac{p-q}{2p}.$$

А такъ какъ по предположенію $p > q$, то $\frac{p-q}{2p}$ есть правильная положительная дробь, и слѣдовательно послѣднему неравенству удовлетворяютъ слѣдующія значенія n:

$$n = 1,\ 2,\ 3, \ldots \frac{q-1}{2}.$$

Отсюда заключаемъ, что въ (6) можно удержать только $\frac{q-1}{2}$ столбцовъ и написать такъ:

$$(7) \ldots M = e\left(\frac{q}{p}\right) + e\left(\frac{q}{2p}\right) + \ldots + e\left(\frac{q}{\frac{q-1}{2}p}\right)$$
$$+ e\left(\frac{2q}{p}\right) + e\left(\frac{2q}{2p}\right) + \ldots + e\left(\frac{2q}{\frac{q-1}{2}p}\right)$$
$$+ e\left(\frac{3q}{p}\right) + e\left(\frac{3q}{2p}\right) + \ldots + e\left(\frac{3q}{\frac{q-1}{2}p}\right)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ e\left(\frac{\frac{p-1}{2}q}{p}\right) + e\left(\frac{\frac{p-1}{2}q}{2p}\right) + \ldots + e\left(\frac{\frac{p-1}{2}q}{\frac{q-1}{2}p}\right).$$

Ни одна изъ дробей подъ знакомъ e въ (7) не равна 1. Ибо полагая

$$lp = mq$$

и замѣчая, что p и q относительно простыя, мы заключаемъ, что l должно дѣлиться на q, а m на p; но ни то, ни другое мѣста не имѣетъ по причинѣ двухъ очевидныхъ неравенствъ:

$$l < q, \quad m < p.$$

Если количество ω не равно 1, то

$$e(\omega) + e\left(\frac{1}{\omega}\right) = 1,$$

отсюда

$$e(\omega) = 1 - e\left(\frac{1}{\omega}\right).$$

По этой формулѣ можно преобразовать каждый членъ въ (7); вслѣдствіе чего на мѣсто (7) получаемъ

$$\begin{aligned}
(8) \qquad M = \frac{(p-1)(q-1)}{4} &- e\left(\frac{p}{q}\right) - e\left(\frac{2p}{q}\right) - \ldots - e\left(\frac{\frac{q-1}{2}p}{q}\right) \\
&- e\left(\frac{p}{2q}\right) - e\left(\frac{2p}{2q}\right) - \ldots - e\left(\frac{\frac{q-1}{2}p}{2q}\right) \\
&- e\left(\frac{p}{3q}\right) - e\left(\frac{2p}{3q}\right) - \ldots - e\left(\frac{\frac{q-1}{2}p}{3q}\right) \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&- e\left(\frac{p}{\frac{p-1}{2}q}\right) - e\left(\frac{2p}{\frac{p-1}{2}q}\right) - \ldots \\
&\qquad - e\left(\frac{\frac{q-1}{2}p}{\frac{p-1}{2}q}\right).
\end{aligned}$$

Слѣдуетъ здѣсь обратить вниманіе на то, что послѣдняя строка во второй части состоитъ изъ однихъ нулей; ибо послѣдняя строка въ (7) состоитъ изъ однихъ единицъ.

Суммируя члены во второй части (8) по столбцамъ, находимъ

$$e\left(\frac{p}{q}\right) + e\left(\frac{p}{2q}\right) + \ldots + e\left(\frac{p}{\frac{p-1}{2}q}\right) = E\frac{p}{q},$$

$$e\left(\frac{2p}{q}\right) + e\left(\frac{2p}{2q}\right) + \ldots + e\left(\frac{2p}{\frac{p-1}{2}q}\right) = E\frac{2p}{q},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$e\left(\frac{\frac{q-1}{2}p}{q}\right) + e\left(\frac{\frac{q-1}{2}p}{2q}\right) + \ldots + e\left(\frac{\frac{q-1}{2}p}{\frac{p-1}{2}q}\right) = E\frac{\frac{q-1}{2}p}{q}.$$

Слѣдовательно

$$M=\frac{p-1}{2}\,\frac{q-1}{2}-E\frac{p}{q}-E\frac{2p}{q}-\ldots-E\frac{\frac{q-1}{2}p}{q}.$$

Внесши это выраженіе въ (5), получаемъ

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}-E\frac{p}{q}-E\frac{2p}{q}-\ldots-E\frac{\frac{q-1}{2}p}{q}},$$

что и требовалось доказать.

Съ помощью двухъ послѣднихъ теоремъ получается новое доказательство закона взаимности простыхъ чиселъ. Дѣйствительно, пусть p и q изображаютъ два какія нибудь различныя простыя числа, оба нечетныя и положительныя, и положимъ $q<p$. По теоремѣ 2-ой имѣемъ

$$\left(\frac{p}{q}\right)=(-1)^{E\frac{p}{q}+E\frac{2p}{q}+\ldots+E\frac{\frac{q-1}{2}p}{q}},$$

а по теоремѣ 3-ей можемъ написать

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}-E\frac{p}{q}-E\frac{2p}{q}-\ldots-E\frac{\frac{q-1}{2}p}{q}}.$$

Перемножая почленно два послѣднія уравненія, находимъ

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}},$$

что совпадаетъ съ теоремой, доказанной въ n^0 50.

52. Съ помощью закона взаимности получается возможность опредѣлять величину какого угодно символа $\left(\frac{q}{p}\right)$. Намъ извѣстно, что на основаніи ранѣе доказанныхъ теоремъ опредѣленіе $\left(\frac{q}{p}\right)$ приводится къ вычисленію одного или нѣсколькихъ символовъ $\left(\frac{r}{p}\right)$, въ которыхъ верхніе члены положительные, нечетные, простые и $<p$. Ко всякому подобному символу примѣнивъ законъ взаимности

Доказательство закона взаимности (продолженіе).

$$\left(\frac{r}{p}\right)=(-1)^{\frac{r-1}{2}\,\frac{p-1}{2}}\left(\frac{p}{r}\right)$$

мы сведемъ вопросъ объ опредѣленіи его величины на вычисленіе обратнаго символа $\left(\frac{p}{r}\right)$, къ которому, въ свою очередь, можно примѣнять опять начальныя теоремы и свести вопросъ на вычисленіе одного или нѣсколькихъ символовъ вида $\left(\frac{r'}{r}\right)$, въ которыхъ верхніе члены положительные, простые, больше 2 и меньше r. Къ этимъ послѣднимъ примѣняемъ вновь законъ взаимности, и продолжаемъ эти дѣйствія до тѣхъ поръ, пока не дойдемъ до символовъ $\left(\frac{1}{r_n}\right)$ или $\left(\frac{2}{r_n}\right)$, которыхъ величину легко найдемъ, а чрезъ нихъ опредѣлится и искомый.

Примѣръ. Пусть будетъ дано найти значеніе $\left(\frac{3153}{1201}\right)$.

Дѣля 3153 на 1201 находимъ въ остаткѣ 751; откуда слѣдуетъ, что

$$\left(\frac{3153}{1201}\right)=\left(\frac{751}{1201}\right).$$

По закону взаимности выводимъ

$$\left(\frac{751}{1201}\right)=(-1)^{\frac{1200}{2}\cdot\frac{750}{2}}\left(\frac{1201}{751}\right)=\left(\frac{1201}{751}\right).$$

Потомъ дѣлимъ 1201 на 751 и получаемъ въ остаткѣ $450=2.\,5^2.\,3^2$. Это даетъ намъ

$$\left(\frac{1201}{751}\right)=\left(\frac{2}{751}\right)=(-1)^{\frac{751^2-1}{8}}=1.$$

Соединяя всѣ эти уравненія, находимъ

$$\left(\frac{3153}{1201}\right)=1.$$

§ III. Символъ Якоби. Его свойства и способъ вычисленія.

53. Единственный недостатокъ вышеизложеннаго способа для опредѣленія величины $\left(\frac{q}{p}\right)$ состоитъ въ могущей встрѣтиться необходимости разложить число на простые множители, что для большихъ чиселъ бываетъ часто весьма затруднительно. Недо-

статокъ этотъ устранилъ Якоби при помощи нѣсколькихъ новыхъ теоремъ, получаемыхъ отъ обобщенія основныхъ свойствъ символа Лежандра.

Обобщеніе это основано на разсматриваніи символа $\left(\frac{Q}{P}\right)$, въ которомъ элементъ P есть число составное, но положительное и нечетное; Q предполагается простымъ съ P.

Полагая

$$P = p_1 p_2 \ldots p_n,$$

гдѣ $p_1, p_2, \ldots p_n$ изображаютъ простые множители, означенный символъ опредѣляемъ по слѣдующей формулѣ:

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\ldots\left(\frac{Q}{p_n}\right),$$

при чемъ множители во второй части представляютъ символы Лежандра. Изъ такого опредѣленія слѣдуетъ, что въ частномъ случаѣ, когда P есть число простое, символъ Якоби совпадаетъ съ символомъ Лежандра; по этой-то причинѣ мы были въ правѣ изобразить символъ Якоби такимъ же знакомъ, какимъ согласились прежде изображать символъ Лежандра.

Прежде чѣмъ приступить къ выводу основныхъ свойствъ новаго символа, докажемъ нижеслѣдующія двѣ леммы.

Лемма 1. *Для всякаго нечетнаго числа*

(1) . . . . $P = p_1 p_2 \ldots p_n$

имѣетъ мѣсто сравненіе

$$\frac{P-1}{2} \equiv \sum_i \frac{p_i - 1}{2} \pmod{2},$$

гдѣ знакъ суммы простирается на значенія $i = 1, 2, \ldots n$.

Въ самомъ дѣлѣ, написавъ уравненіе (1) такъ:

$$P = (1 + (p_1 - 1))\,(1 + (p_2 - 1)) \ldots (1 + (p_n - 1)),$$

перемножимъ между собою двучлены во второй части; получаемъ

$$P = 1 + \Sigma_i (p_i - 1) + \Sigma_{i,j} (p_i - 1)(p_j - 1) + \ldots,$$

гдѣ знаки суммы простираются соотвѣтственно на всѣ произведенія элементовъ $p_1 - 1, p_2 - 1, \ldots p_n - 1$ по одному, по два и т. д. А такъ какъ каждый изъ означенныхъ элементовъ есть число четное, то каждое ихъ произведеніе по два даетъ число дѣлящееся на 4; вслѣдствіе этого послѣднее уравненіе приводитъ къ слѣдующему сравненію

$$P - 1 \equiv \Sigma_i (p_i - 1) \pmod{4}.$$

Здѣсь обѣ части, равно какъ и модуль, дѣлятся на 2; поэтому выводимъ

$$\frac{P-1}{2} \equiv \sum_i \frac{p_i - 1}{2} \pmod{2},$$

что и слѣдовало доказать.

Лемма 2. *Для всякаго нечетнаго числа*

$$P = p_1 p_2 \ldots p_n$$

имѣетъ мѣсто сравненіе

$$\frac{P^2-1}{8} \equiv \sum_i \frac{p_i^2 - 1}{8} \pmod{2}.$$

Для доказательства представимъ P^2 въ такомъ видѣ:

$$P^2 = (1 + (p_1^2 - 1))(1 + (p_2^2 - 1)) \ldots (1 + (p_n^2 - 1)),$$

и перемножимъ между собою двучлены во второй части; получаемъ

$$P^2 = 1 + \Sigma (p_i^2 - 1) + \Sigma (p_i^2 - 1)(p_j^2 - 1) + \ldots$$

Такъ какъ числа $p_1, p_2, \ldots p_n$ по предположенію суть нечетныя, то каждый изъ элементовъ

$$p_1^2 - 1,\ p_2^2 - 1, \ldots p_n^2 - 1$$

дѣлится на 8, вслѣдствіе чего изъ послѣдняго уравненія заключаемъ

$$P^2-1\equiv\Sigma(p_i^2-1)\ (\mathrm{mod.}\ 64).$$

Обѣ части, равно какъ и модуль, послѣдняго сравненія дѣлятся на 8; послѣ сокращенія получаемъ

$$\frac{P^2-1}{8}\equiv\sum_i\frac{p_i^2-1}{8}\ (\mathrm{mod.}\ 8),$$

или подавно

$$\frac{P^2-1}{8}\equiv\sum_i\frac{p_i^2-1}{8}\ (\mathrm{mod.}\ 2),$$

что и требовалось доказать.

54. Докажемъ теперь, что символъ $\left(\frac{Q}{P}\right)$ удовлетворяетъ всѣмъ тѣмъ уравненіямъ, которыя служили намъ для опредѣленія величины символа $\left(\frac{q}{p}\right)$ при p простомъ.

Теорема 1. *Величины* $\left(\frac{1}{P}\right)$ *и* $\left(\frac{-1}{P}\right)$ *при P сложномъ опредѣляются точно также какъ и при P простомъ, именно:*

$$\left(\frac{1}{P}\right)=1,\ \left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}.$$

Въ самомъ дѣлѣ, полагая $P=p_1\,p_2\ldots p_n$, гдѣ $p_1,p_2,\ldots p_n$ простыя числа, имѣемъ

$$\left(\frac{1}{P}\right)=\left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\ldots\left(\frac{1}{p_n}\right),\ \left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\ldots\left(\frac{-1}{p_n}\right),$$

откуда заключаемъ

$$\left(\frac{1}{P}\right)=1,\ \left(\frac{-1}{P}\right)=(-1)^{\sum_i\frac{p_i-1}{2}}.$$

На основаніи первой леммы, доказанной въ предыдущемъ номерѣ, имѣемъ

$$\frac{P-1}{2}=\sum\frac{p_i-1}{2}+2l,$$

гдѣ l число цѣлое; слѣдовательно

$$(-1)^{\sum_i\frac{p_i-1}{2}}=(-1)^{\frac{P-1}{2}-2l}=(-1)^{\frac{P-1}{2}}.$$

Внося это выраженіе на мѣсто второй части въ предыдущую формулу находимъ

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}},$$

что и слѣдовало доказать.

Слѣдствіе. *Если P есть вида* $4m+1$, *то* $\left(\frac{-1}{P}\right)=1$; *если же P есть вида* $4m+3$, *то* $\left(\frac{-1}{P}\right)=-1$.

Теорема 2. *Если Q равно произведенію чиселъ* $q_1, q_2, \ldots q_m$, *то*

$$\left(\frac{Q}{P}\right)=\left(\frac{q_1}{P}\right)\left(\frac{q_2}{P}\right)\ldots\left(\frac{q_m}{P}\right).$$

Дѣйствительно, полагая $P=p_1\,p_2\ldots p_n$, гдѣ $p_1, p_2, \ldots p_n$ простыя числа, имѣемъ

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\ldots\left(\frac{Q}{p_n}\right).$$

Съ другой стороны, по свойству символа Лежандра, имѣемъ

$$\left(\frac{Q}{p_1}\right)=\left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)\ldots\left(\frac{q_m}{p_1}\right),$$

$$\left(\frac{Q}{p_2}\right)=\left(\frac{q_1}{p_2}\right)\left(\frac{q_2}{p_2}\right)\ldots\left(\frac{q_m}{p_2}\right),$$

. . . .

. . . .

$$\left(\frac{Q}{p_n}\right)=\left(\frac{q_1}{p_n}\right)\left(\frac{q_2}{p_n}\right)\ldots\left(\frac{q_m}{p_n}\right).$$

Перемножая эти уравненія между собою и замѣчая, что произведеніе всѣхъ множителей во вторыхъ частяхъ, образующихъ i-ой столбецъ, есть

$$\left(\frac{q_i}{p_1}\right)\left(\frac{q_i}{p_2}\right)\ldots\left(\frac{q_i}{p_n}\right)=\left(\frac{q_i}{P}\right),$$

находимъ

$$\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\ldots\left(\frac{Q}{p_n}\right)=\left(\frac{q_1}{P}\right)\left(\frac{q_2}{P}\right)\ldots\left(\frac{q_m}{P}\right).$$

Сличая это уравненіе съ предшествующимъ выраженіемъ для $\left(\frac{Q}{P}\right)$, получаемъ

$$\left(\frac{Q}{P}\right)=\left(\frac{q_1}{P}\right)\left(\frac{q_2}{P}\right)\cdots\left(\frac{q_m}{P}\right),$$

что и требовалось доказать.

Слѣдствіе. *Въ символѣ $\left(\frac{Q}{P}\right)$ можно выкидывать изъ состава Q точные квадраты.*

Теорема. *Величина символа $\left(\frac{2}{P}\right)$ опредѣляется по формулѣ*

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

Дѣйствительно, полагая, какъ прежде, $P=p_1 p_2 \ldots p_n$, гдѣ $p_1, p_2, \ldots$ числа простыя, имѣемъ

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_n}\right),$$

откуда заключаемъ

$$\left(\frac{2}{P}\right)=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_n^2-1}{8}}=(-1)^{\sum\frac{p_i^2-1}{8}}.$$

Но на основаніи второй леммы предыдущаго номера имѣемъ

$$\sum\frac{p_i^2-1}{8}\equiv\frac{P^2-1}{8}\ (\text{mod. } 2).$$

Сравненіе это показываетъ, что обѣ его части суть одновременно четныя или нечетныя; поэтому имѣетъ мѣсто уравненіе

$$(-1)^{\sum\frac{p_i^2-1}{8}}=(-1)^{\frac{P^2-1}{8}}.$$

Соединяя это уравненіе съ предшествующимъ, заключаемъ

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}},$$

что и слѣдовало доказать.

Слѣдствіе. *Если P есть вида* $8n \pm 1$, *то* $\left(\frac{2}{P}\right) = 1$; *если же оно вида* $8n \pm 3$, *то* $\left(\frac{2}{P}\right) = -1$.

Теорема 3. *Если числа Q и Q' сравнимы по модулю P, то*

$$\left(\frac{Q}{P}\right) = \left(\frac{Q'}{P}\right).$$

Дѣйствительно, полагая $P = p_1 p_2 \ldots p_n$, гдѣ $p_1, p_2, \ldots$ числа простыя, имѣемъ рядъ сравненій

$$Q \equiv Q' \ (\text{mod.}\ p_1),$$

$$Q \equiv Q' \ (\text{mod.}\ p_2),$$

$$\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots$$

$$Q \equiv Q' \ (\text{mod.}\ p_n),$$

на основаніи которыхъ заключаемъ

$$\left(\frac{Q}{p_1}\right) = \left(\frac{Q'}{p_1}\right),$$

$$\left(\frac{Q}{p_2}\right) = \left(\frac{Q'}{p_2}\right),$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$\left(\frac{Q}{p_n}\right) = \left(\frac{Q'}{p_n}\right).$$

Перемножая между собою всѣ эти уравненія и замѣчая, что произведеніе первыхъ частей представляетъ величину символа $\left(\frac{Q}{P}\right)$, а вторыхъ частей — величину символа $\left(\frac{Q'}{P}\right)$, получаемъ

$$\left(\frac{Q}{P}\right) = \left(\frac{Q'}{P}\right),$$

что и требовалось доказать.

Теорема 4. *Если P и Q суть числа относительно простыя, оба положительныя и нечетныя, то*

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

На самомъ дѣлѣ, положивъ $P=p_1 p_2 \ldots p_n$, $Q=q_1 q_2 \ldots q_m$, гдѣ $p_1, p_2, \ldots q_1, q_2, \ldots$ числа простыя, имѣемъ

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\ldots\left(\frac{Q}{p_n}\right)=\left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)\ldots\left(\frac{q_m}{p_1}\right)$$
$$\left(\frac{q_1}{p_2}\right)\left(\frac{q_2}{p_2}\right)\ldots\left(\frac{q_m}{p_2}\right)$$
$$\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots$$
$$\left(\frac{q_1}{p_n}\right)\left(\frac{q_2}{p_n}\right)\ldots\left(\frac{q_m}{p_n}\right).$$

Уравненіе это можно написать такъ:

$$\left(\frac{Q}{P}\right)=\prod_{i,j}\left(\frac{q_j}{p_i}\right),$$

причемъ знакъ произведенія простирается на значенія

$$i=1, 2, 3, \ldots n,$$
$$j=1, 2, 3, \ldots m.$$

По закону взаимности простыхъ чиселъ имѣемъ

$$\left(\frac{q_j}{p_i}\right)=\left(\frac{p_i}{q_j}\right)(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}.$$

Внося это выраженіе во вторую часть предыдущаго уравненія, получаемъ

$$\left(\frac{Q}{P}\right)=\prod_{i,j}\left(\frac{p_i}{q_j}\right)(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}},$$

или

$$\left(\frac{Q}{P}\right)=\prod_{i,j}\left(\frac{p_i}{q_j}\right)\prod_{i,j}(-1)^{\frac{p_i-1}{2}\,\frac{q_j-1}{2}}.$$

Разсматривая здѣсь вторую часть, какъ произведенíе двухъ множителей, мы замѣчаемъ, что первый множитель представляетъ величину символа $\left(\frac{P}{Q}\right)$, второй равенъ

$$(-1)^{\sum\frac{p_i-1}{2}\,\frac{q_j-1}{2}},$$

гдѣ знакъ суммы простирается на всѣ значенія значковъ i и j. Слѣдовательно

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)(-1)^{\sum\frac{p_i-1}{2}\,\frac{q_j-1}{2}}.$$

Сумма во второй части разлагается на произведенíе двухъ многочленовъ

$$\sum_{i,j}\frac{p_i-1}{2}\,\frac{q_j-1}{2}=\sum_i\frac{p_i-1}{2}\sum_j\frac{q_j-1}{2};$$

поэтому можно написать

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)(-1)^{\sum\frac{p_i-1}{2}\sum\frac{q_j-1}{2}}.$$

Но по первой леммѣ, доказанной въ предшествующемъ номерѣ, имѣемъ

$$\sum_i\frac{p_i-1}{2}\equiv\frac{P-1}{2}\ (\mathrm{mod.}\ 2),$$

$$\sum_j\frac{q_j-1}{2}\equiv\frac{Q-1}{2}\ (\mathrm{mod.}\ 2),$$

откуда выходитъ

$$\sum_i\frac{p_i-1}{2}\sum_j\frac{q_j-1}{2}\equiv\frac{P-1}{2}\,\frac{Q-1}{2}\ (\mathrm{mod.}\ 2).$$

Это сравненіе показываетъ, что обѣ его части суть четныя или нечетныя одновременно; поэтому имѣемъ

$$(-1)^{\sum\frac{p_i-1}{2}\sum\frac{q_j-1}{2}}=(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Внося въ предшествующее выраженіе символа $\left(\frac{Q}{P}\right)$ на мѣсто втораго множителя только что полученное, равное значеніе, находимъ

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)(-1)^{\frac{P-1}{2}\frac{Q-1}{2}},$$

что и слѣдовало доказать.

Слѣдствіе. *Если по крайней мѣрѣ одно изъ чиселъ* P, Q *есть вида* $4n+1$, *то*

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right);$$

если же оба они вида $4n+3$, *то*

$$\left(\frac{Q}{P}\right)=-\left(\frac{P}{Q}\right).$$

55. На основаніи всего вышеизложеннаго, чтобы опредѣлить величину символа $\left(\frac{Q}{P}\right)$, во всякомъ частномъ случаѣ можно поступать слѣдующимъ образомъ.

Найдемъ абсолютно малый вычетъ числа Q по модулю P и представимъ его такъ:

$$(-1)^{a_1}2^{b_1}r_1,$$

гдѣ a_1 равно нулю или 1, b_1 можетъ равняться нулю, r_1 число нечетное и положительное.

Послѣ этого, если $r_1>1$, находимъ абсолютно малый вычетъ числа P по модулю r_1 и представляемъ его такъ:

$$(-1)^{a_2}2^{b_2}r_2.$$

Затѣмъ, если $r_2 > 1$, находимъ абсолютно малый вычетъ числа r_1 по модулю r_2 и, подобно предыдущему, представляемъ его въ видѣ

$$(-1)^{a_3} 2^{b_3} r_3.$$

Такимъ образомъ слѣдуетъ дѣйствовать до тѣхъ поръ, пока не дойдемъ до $r_n = 1$. Полученнымъ такимъ образомъ вычетамъ соотвѣтствуетъ рядъ уравненій

$$\left(\frac{Q}{P}\right) = (-1)^{a_1 \frac{P-1}{2} + b_1 \frac{P^2-1}{8} + \frac{P-1}{2} \frac{r_1-1}{2}} \left(\frac{P}{r_1}\right),$$

$$\left(\frac{P}{r_1}\right) = (-1)^{a_2 \frac{r_1-1}{2} + b_2 \frac{r_1^2-1}{8} + \frac{r_1-1}{2} \frac{r_2-1}{2}} \left(\frac{r_1}{r_2}\right),$$

. . . .

. . . .

$$\left(\frac{r_{n-2}}{r_{n-1}}\right) = (-1)^{a_n \frac{r_{n-1}-1}{2} + b_n \frac{r^2_{n-1}-1}{8}}.$$

Отсюда величина $\left(\frac{Q}{P}\right)$ получается непосредственно.

Символъ Лежандра, будучи разсматриваемъ, какъ частный случай символа Якоби, можетъ быть вычисляемъ по сейчасъ указанному способу, при чемъ мы избавлены отъ необходимости разлагать числа на простые множители.

Примѣръ. Пусть дано будетъ опредѣлить значеніе $\left(\frac{2251}{5939}\right)$.

На основаніи закона взаимности выводимъ

$$\left(\frac{2251}{5939}\right) = -\left(\frac{5939}{2251}\right).$$

Дѣля 5939 на 2251 и находя въ остаткѣ -814, заключаемъ, что

$$\left(\frac{5939}{2251}\right) = \left(\frac{-1}{2251}\right)\left(\frac{2}{2251}\right)\left(\frac{407}{2251}\right) = \left(\frac{407}{2251}\right).$$

Но опять на основаніи закона взаимности находимъ

$$\left(\frac{407}{2251}\right) = -\left(\frac{2251}{407}\right).$$

Дѣля 2251 на 407 и находя въ остаткѣ —191, заключаемъ, что

$$\left(\frac{2251}{407}\right)=\left(\frac{-1}{407}\right)\left(\frac{191}{407}\right)=-\left(\frac{191}{407}\right).$$

Продолжая такимъ образомъ, выводимъ

$$\left(\frac{191}{407}\right)=-\left(\frac{407}{191}\right)=-\left(\frac{25}{191}\right)=-\left(\frac{5^2}{191}\right)=-1.$$

Соединяя полученныя уравненія, находимъ

$$\left(\frac{2251}{5939}\right)=1.$$

§ IV. Рѣшеніе сравненія $x^2 \equiv q \pmod{p}$ въ нѣкоторыхъ частныхъ случаяхъ.

56. Послѣ того, какъ мы научились узнавать, возможно ли сравненіе

$$x^2 \equiv q \pmod{p}$$

или нѣтъ, намъ слѣдовало бы заняться способами нахожденія самаго рѣшенія, когда оно существуетъ. Но вопросъ этотъ остается открытымъ. За исключеніемъ нѣкоторыхъ частныхъ случаевъ, мы не имѣемъ ни общей формулы для искомаго рѣшенія, ни удобнаго способа для вычисленія его; вообще говоря, приходится во всякомъ частномъ случаѣ или испытывать поочередно всѣ числа не превышающія половины модуля, или же пользоваться специальными таблицами, употребленіе которыхъ будетъ объяснено впослѣдствіи.

Между частными случаями заслуживаетъ вниманія сравненіе

$$x^2 \equiv -1 \pmod{p},$$

когда модуль есть вида $4n+1$; тогда имѣемъ

$$x \equiv \pm 1.\,2.\,3\ldots\frac{p-1}{2} \pmod{p},$$

что очевидно на основаніи теоремы Вильсона.

Случай, когда модуль есть вида $4n+3$, не представляетъ никакихъ затрудненій относительно явнаго выраженія корней сравненія

(1) . . . . $x^2 \equiv q \pmod{p}$;

тогда имѣемъ

(2) . . . . $x \equiv \pm q^{\frac{p+1}{4}} \pmod{p}$,

при чемъ, конечно, предполагается, что $\left(\frac{q}{p}\right) = 1$.

Чтобы провѣрить справедливость вышесказаннаго, возвышаемъ обѣ части (2) въ квадратъ; получаемъ

$$x^2 \equiv q^{\frac{p+1}{2}} \pmod{p},$$

что можно написать такъ:

$$x^2 \equiv q^{\frac{p-1}{2}} q \pmod{p}.$$

Но

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p};$$

слѣдовательно

$$x^2 \equiv \left(\frac{q}{p}\right) q \pmod{p};$$

а такъ какъ

$$\left(\frac{q}{p}\right) = 1,$$

то окончательно получаемъ

$$x^2 \equiv q \pmod{p}.$$

Это показываетъ, что формула (2) опредѣляетъ дѣйствительно корни сравненія (1).

ГЛАВА V.

О квадратичныхъ вычетахъ и невычетахъ. — О дѣлителяхъ формы $t^2 - Du^2$.

§ 1. О квадратичныхъ вычетахъ.

57. Число q, простое съ p, называется *квадратичнымъ вычетомъ* послѣдняго, когда сравненіе

$$x^2 \equiv q \pmod{p}$$

имѣетъ рѣшеніе; въ противномъ случаѣ q называется *квадратичнымъ невычетомъ* числа p.

Очевидно, что числа сравнимыя по модулю p суть одновременно или квадратичные вычеты или квадратичные невычеты.

Всѣ квадратичные вычеты *простаго* числа p суть корни сравненія

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

или, что одно и то же, корни уравненія

$$\left(\frac{x}{p}\right) = 1.$$

Всѣ квадратичные невычеты *простаго* числа p удовлетворяютъ сравненію

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

или, что одно и то же, уравненію

$$\left(\frac{x}{p}\right) = -1:$$

Половина чиселъ въ ряду

$$1, 2, 3, \ldots p-1$$

суть квадратичные вычеты, половина квадратичные невычеты (см. n^0 46). Первыя будемъ изображать буквами $a_1, a_2, \ldots a_{\frac{p-1}{2}}$, вторыя буквами $b_1, b_2, \ldots b_{\frac{p-1}{2}}$.

Изъ свойства символа Лежандра, по которому имѣемъ

$$\left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right) = \left(\frac{qq_1}{p}\right),$$

вытекаютъ слѣдующія предложенія.

1°. *Произведеніе двухъ квадратичныхъ вычетовъ $a_i\, a_j$ есть также квадратичный вычетъ.*

2°. *Произведеніе двухъ квадратичныхъ невычетовъ $b_i\, b_j$ есть квадратичный вычетъ.*

3°. *Произведеніе $a_i\, b_j$ квадратичнаго вычета на квадратичный невычетъ есть квадратичный невычетъ.*

Примѣръ. Положимъ $p = 13$. Чтобы получить всѣ квадратичные вычеты этого числа, мы дѣлимъ точные квадраты 1, 4, 16, 25, 36 на 13; остатки

$$1,\ 4,\ 9,\ 3,\ 12,\ 10$$

суть искомые квадратичные вычеты. Числа не содержащіяся въ послѣднемъ ряду, именно:

$$2,\ 5,\ 6,\ 7,\ 8,\ 11$$

суть квадратичные невычеты. Справедливость послѣднихъ предложеній провѣряется непосредственно.

58. Та опредѣленная связь, которая существуетъ между значеніемъ символа $\left(\frac{q}{p}\right)$ и возможностью сравненія $x^2 \equiv q \pmod{p}$, исчезаетъ при сложномъ модулѣ. Положивъ $P = p_1 p_2 \ldots p_n$, гдѣ $p_1, p_2, \ldots$ числа простыя, и допустивъ, что сравненіе

$$(1) \ldots\ldots\ldots\ldots\ldots x^2 \equiv q \ (\text{mod.}\ P)$$

имѣетъ рѣшеніе, мы заключаемъ, что x будетъ удовлетворять каждому изъ сравненій

$$x^2 \equiv q \ (\text{mod.}\ p_1),$$
$$x^2 \equiv q \ (\text{mod.}\ p_2),$$
$$\ldots\ldots\ldots\ldots$$
$$x^2 \equiv q \ (\text{mod.}\ p_n);$$

слѣдовательно будутъ имѣть мѣсто уравненія

$$(2) \ldots\ldots \left(\frac{q}{p_1}\right) = 1,\ \left(\frac{q}{p_2}\right) = 1, \ldots \left(\frac{q}{p_n}\right) = 1,$$

по перемноженіи которыхъ получаемъ

$$(3) \ldots\ldots\ldots\ldots\ldots \left(\frac{q}{P}\right) = 1.$$

Это, какъ видимъ, есть условіе *необходимое* для того, чтобы сравненіе (1) было возможно; оно одинаково, какъ при простомъ P, такъ и при сложномъ. Разница обнаруживается, когда поставленъ вопросъ о *достаточности* условія (3): при сложномъ P уравненіе (3) можетъ быть удовлетворено, между тѣмъ какъ нѣкоторыя изъ (2) не будутъ имѣть мѣста; тогда сравненіе (1) очевидно невозможно.

Итакъ, изъ вышесказаннаго слѣдуетъ, *что всѣ квадратичные вычеты числа P заключаются между рѣшеніями уравненія* $\left(\frac{x}{P}\right) = 1$.

59. Разсматривая рѣшенія какого нибудь изъ уравненій

$$(1) \ldots\ldots\ldots\ldots \left(\frac{x}{P}\right)=1,\ \left(\frac{x}{P}\right)=-1,$$

мы согласимся не считать за различныя такія рѣшенія, которыя сравнимы по модулю P; такъ что число рѣшеній опредѣлится числомъ чиселъ въ ряду

$$1,\ 2,\ 3, \ldots P-1,$$

простыхъ съ P и удовлетворяющихъ разсматриваемому уравненію.

Такъ какъ символъ $\left(\frac{x}{P}\right)$ не измѣняетъ своего значенія если изъ состава P выкинуть точный квадратъ, то относительно каждаго изъ уравненій (1) можно ограничиться предположеніемъ, что P не дѣлится ни на какой квадратъ. Но пока еще намъ нѣтъ необходимости вводить такое допущеніе.

Если P есть точный квадратъ, то уравненію

$$\left(\frac{x}{P}\right)=1$$

удовлетворяетъ всякое значеніе x; напротивъ, уравненіе

$$\left(\frac{x}{P}\right)=-1$$

не имѣетъ вовсе рѣшенія.

Остается предполагать, что P не есть точный квадратъ. Тогда имѣетъ мѣсто слѣдующая теорема.

Теорема. *Если P не есть точный квадратъ, то оба уравненія*

$$\left(\frac{x}{P}\right)=1 \quad \text{и} \quad \left(\frac{x}{P}\right)=-1$$

имѣютъ по одинаковому числу рѣшеній, именно по $\frac{1}{2}\varphi(P)$.

Если P число простое, теорема не представляетъ тогда ничего новаго; она повторяетъ то, что было нами изложено въ n^0 57.

Предполагая P числомъ сложнымъ, мы обозначимъ чрезъ p одинъ изъ простыхъ множителей, входящихъ въ составъ P съ нечетнымъ показателемъ; пусть

$$P = p^m P',$$

гдѣ P' не дѣлится на p.

Возьмемъ во вниманіе какой нибудь невычетъ числа p, обозначимъ его чрезъ b, и отыщемъ число c, которое удовлетворяло бы такимъ двумъ сравненіямъ:

$$c \equiv b \ (\text{mod.}\, p), \quad c \equiv 1 \ (\text{mod.}\, P').$$

Очевидно, что c будетъ простое съ P, и будемъ имѣть

$$\left(\frac{c}{P}\right) = \left(\frac{c}{p^m P'}\right) = \left(\frac{c}{p}\right)^m \left(\frac{c}{P'}\right) = \left(\frac{b}{p}\right)^m \left(\frac{1}{P'}\right) = (-1)^m;$$

а такъ какъ m число нечетное, то слѣдовательно

$$\left(\frac{c}{P}\right) = -1.$$

Такимъ образомъ мы нашли одно рѣшеніе уравненія

$$\left(\frac{x}{P}\right) = -1.$$

Но какъ только извѣстно, что это уравненіе имѣетъ одно рѣшеніе, сейчасъ можно показать, что оно имѣетъ ихъ ровно $\frac{1}{2}\varphi(P)$.

Въ самомъ дѣлѣ, обозначивъ чрезъ y наименьшій положительный вычетъ произведенія cx по модулю P, мы замѣчаемъ, что если x простое съ P, y также простое съ P, и если x будетъ поочередно получать всѣ $\varphi(P)$ значеній, простыхъ съ P и $< P$, число y пройдетъ послѣдовательно чрезъ тѣ же значенія. Вслѣдствіе этого имѣемъ уравненіе

$$\sum \left(\frac{x}{P}\right) = \sum \left(\frac{y}{P}\right);$$

а такъ какъ

$$\left(\frac{cx}{P}\right)=\left(\frac{y}{P}\right),$$

то слѣдовательно

$$\sum\left(\frac{cx}{P}\right)=\sum\left(\frac{x}{P}\right),$$

при чемъ знакъ суммы въ обѣихъ частяхъ простирается на всѣ значенія x, простыя съ P и $<P$.

Подставляя въ первой части $\left(\frac{c}{P}\right)\left(\frac{x}{P}\right)$ на мѣсто $\left(\frac{cx}{P}\right)$ и вынося общій множитель за знакъ суммы, получаемъ

$$\left(\frac{c}{P}\right)\sum\left(\frac{x}{P}\right)=\sum\left(\frac{x}{P}\right)$$

или, подставивъ -1 на мѣсто $\left(\frac{c}{P}\right)$,

$$-\sum\left(\frac{x}{P}\right)=\sum\left(\frac{x}{P}\right);$$

отсюда выводимъ

(2) . . . . $\sum\left(\frac{x}{P}\right)=0.$

Если обозначимъ чрезъ m число рѣшеній уравненія

$$\left(\frac{x}{P}\right)=1,$$

а чрезъ m' число рѣшеній уравненія

$$\left(\frac{x}{P}\right)=-1,$$

уравненіе (2) можно написать такъ:

$$m-m'=0.$$

Съ другой стороны, имѣемъ очевидно

$$m+m'=\varphi(P).$$

Изъ двухъ послѣднихъ уравненій выводимъ

$$m=m'=\tfrac{1}{2}\varphi(P),$$

что и слѣдовало доказать.

Примѣръ. Рѣшенія уравненія $\left(\frac{x}{15}\right)=1$ суть слѣдующія:

$$x=1,\ 2,\ 4,\ 8,$$

а уравненія $\left(\frac{x}{15}\right)=-1$:

$$x=7,\ 11,\ 13,\ 14.$$

§ II. О рѣшеніяхъ уравненія $\left(\frac{D}{x}\right)=\pm 1$ и о дѣлителяхъ формы t^2-Du^2.

60. Разсматривая символъ $\left(\frac{D}{x}\right)$, мы постоянно будемъ подразумѣвать, что D не есть точный квадратъ; иначе значеніе символа не зависѣло бы отъ x и всегда равнялось бы 1. При $x=1$ согласимся принимать $\left(\frac{D}{1}\right)=1$.

Представивъ D въ видѣ

$$D=(-1)^a 2^b Q,$$

гдѣ a есть нуль или 1, b можетъ равняться нулю, а Q есть число положительное и нечетное, имѣемъ равенство

$$\left(\frac{D}{x}\right)=\left(\frac{-1}{x}\right)^a\left(\frac{2}{x}\right)^b\left(\frac{Q}{x}\right)=(-1)^{a\frac{x-1}{2}}(-1)^{b\frac{x^2-1}{2}}\left(\frac{Q}{x}\right).$$

Но по закону взаимности

$$\left(\frac{Q}{x}\right)=(-1)^{\frac{Q-1}{2}\frac{x-1}{2}}\left(\frac{x}{Q}\right);$$

слѣдовательно

$$\left(\frac{D}{x}\right)=(-1)^{\frac{x-1}{2}\left(a+\frac{Q-1}{2}\right)+b\frac{x^2-1}{8}}\left(\frac{x}{Q}\right).$$

Дѣлая для сокращенія

$$\delta=(-1)^{a+\frac{Q-1}{2}},\quad \varepsilon=(-1)^b,$$

получаемъ

$$(1) \ldots\ldots\ldots\ldots \left(\frac{D}{x}\right) = \delta^{\frac{x-1}{2}} \varepsilon^{\frac{x^2-1}{8}} \left(\frac{x}{Q}\right),$$

при чемъ ε равно 1 или —1, смотря по тому будетъ ли b четное или нечетное; δ равно 1 или —1, смотря по тому будетъ ли частное $\frac{D}{2^b}$ вида $4n+1$ или $4n-1$.

Съ помощью (1) легко убѣдиться въ справедливости нижеслѣдующихъ двухъ теоремъ.

Теорема 1. *Величина* $\left(\frac{D}{x}\right)$, *будучи разсматриваема какъ функція* x, *есть періодическая, съ періодомъ* $4D$.

Дѣйствительно, внося въ обѣ части (1) $x+4D$ на мѣсто x, получаемъ

$$\left(\frac{D}{x+4D}\right) = \delta^{\frac{x-1}{2}+2D} \varepsilon^{\frac{x^2-1}{8}+xD+2D^2} \left(\frac{x+4D}{Q}\right).$$

Здѣсь во второй части, въ показателяхъ, можно отбросить члены $2D$ и $2D^2$, какъ четные и не имѣющіе потому вліянія на значенія соотвѣтствующихъ множителей; можно слѣдовательно написать проще

$$\left(\frac{D}{x+4D}\right) = \delta^{\frac{x-1}{2}} \varepsilon^{\frac{x^2-1}{8}} \varepsilon^{xD} \left(\frac{x+4D}{Q}\right).$$

Но $x+4D \equiv x \pmod{Q}$; поэтому

$$\left(\frac{x+4D}{Q}\right) = \left(\frac{x}{Q}\right),$$

и слѣдовательно

$$\left(\frac{D}{x+4D}\right) = \delta^{\frac{x-1}{2}} \varepsilon^{\frac{x^2-1}{8}} \varepsilon^{xD} \left(\frac{x}{Q}\right).$$

Наконецъ мы замѣчаемъ, что

$$\varepsilon^{xD} = 1;$$

ибо ε тогда только равно -1, когда D четное. Вслѣдствіе этого получаемъ

$$(2) \ldots\ldots\ldots\ldots \left(\frac{D}{x+4D}\right)=\delta^{\frac{x-1}{2}}\varepsilon^{\frac{x^2-1}{8}}\left(\frac{x}{Q}\right).$$

Изъ (1) и (2) выводимъ

$$\left(\frac{D}{x}\right)=\left(\frac{D}{x+4D}\right),$$

что и слѣдовало доказать.

Слѣдствіе. *Если* $x\equiv x'$ (mod. $4D$), *то*

$$\left(\frac{D}{x}\right)=\left(\frac{D}{x'}\right).$$

Теорема 2. *Если* $D\equiv 1$ (mod. 4), *то величина символа* $\left(\frac{D}{x}\right)$ *представляетъ періодическую функцію перемѣннаго x съ періодомъ* $2D$.

Дѣйствительно, въ предполагаемомъ случаѣ имѣемъ $\varepsilon=\delta=1$; вслѣдствіе этого равенство (1) принимаетъ видъ

$$(3) \ldots\ldots\ldots\ldots \left(\frac{D}{x}\right)=\left(\frac{x}{Q}\right),$$

при чемъ Q представляетъ числовую величину D.

Подставляя въ обѣихъ частяхъ (3) $x+2D$ на мѣсто x и замѣчая, что

$$\left(\frac{x+2D}{Q}\right)=\left(\frac{x}{Q}\right),$$

получаемъ

$$(4) \ldots\ldots\ldots\ldots \left(\frac{D}{x+2D}\right)=\left(\frac{x}{Q}\right).$$

Изъ (3) и (4) выводимъ

$$\left(\frac{D}{x}\right)=\left(\frac{D}{x+2D}\right),$$

что и слѣдовало доказать.

Слѣдствіе. *Если* $D \equiv 1 \pmod{4}$ *и* $x \equiv x' \pmod{2D}$, *то*

$$\left(\frac{D}{x}\right) = \left(\frac{D}{x'}\right).$$

61. Изъ вышедоказаннаго слѣдуетъ, что если a удовлетворяетъ одному изъ уравненій

$$\left(\frac{D}{x}\right) = 1, \ \left(\frac{D}{x}\right) = -1,$$

то тому же уравненію будутъ удовлетворять всѣ прочія числа, сравнимыя съ a по модулю $4D$. Поэтому мы согласимся для каждаго изъ означенныхъ уравненій рѣшенія, сравнимыя между собою по модулю $4D$, не считать за различныя; и будемъ говорить, что каждое изъ этихъ уравненій имѣетъ столько рѣшеній, сколько существуетъ чиселъ въ ряду

$$1, 3, 5, \ldots 4D - 1,$$

удовлетворяющихъ ему и, конечно, простыхъ съ D.

Уравненіе $\left(\frac{D}{x}\right) = 1$ имѣетъ всегда рѣшеніе; это очевидно, ибо $\left(\frac{D}{1}\right) = 1$. То же самое можно сказать и объ уравненіи $\left(\frac{D}{x}\right) = -1$; но только здѣсь это не очевидно: необходимо доказать справедливость предложенія.

Для этого допустимъ сначала, что въ выраженіи

$$D = (-1)^a 2^b Q$$

множитель Q не есть точный квадратъ, и обозначивъ чрезъ h какое нибудь изъ чиселъ, удовлетворяющихъ условію

$$\left(\frac{h}{Q}\right) = -1,$$

найдемъ число c, которое удовлетворяло бы двумъ такимъ сравненіямъ:

$$c \equiv h \pmod{Q}$$

$$c \equiv 1 \pmod{8}.$$

Внося въ равенство (1) n^0 60 c на мѣсто x, находимъ

$$\left(\frac{D}{c}\right)=\delta^{\frac{c-1}{2}}\varepsilon^{\frac{c^2-1}{8}}\left(\frac{c}{Q}\right)=\left(\frac{c}{Q}\right)=\left(\frac{h}{Q}\right)=-1.$$

Слѣдовательно, въ предполагаемомъ случаѣ уравненію $\left(\frac{D}{x}\right)=-1$ удовлетворяетъ число $x=c$. Остается доказать справедливость предложенія въ томъ случаѣ, когда множитель Q есть полный квадратъ.

Тогда имѣетъ мѣсто равенство

$$\left(\frac{D}{x}\right)=\delta^{\frac{x-1}{2}}\varepsilon^{\frac{x^2-1}{8}},$$

и не можетъ случиться, чтобы одновременно оба числа δ и ε равнялись 1; ибо, по предположенію, D не есть точный квадратъ. Слѣдовательно, возможны только слѣдующія предположенія:

$$\delta=-1,\quad \varepsilon=1;$$

$$\delta=1,\quad \varepsilon=-1;$$

$$\delta=-1,\quad \varepsilon=-1.$$

Въ первыхъ двухъ имѣемъ

$$\left(\frac{D}{4Q-1}\right)=-1,$$

а въ третьемъ

$$\left(\frac{D}{4Q+1}\right)=-1.$$

Итакъ, каково бы ни было D, уравненіе $\left(\frac{D}{x}\right)=-1$ всегда возможно.

Съ помощью вышеизложеннаго легко доказать слѣдующую теорему.

Теорема 1. *Между числами, простыми относительно* $4D$ *и не превышающими числовой величины* $4D$, *половина удовлетворяетъ уравненію*

$$\left(\frac{D}{x}\right)=1,$$

остальная половина — уравненію

$$\left(\frac{D}{x}\right) = -1.$$

Дѣйствительно, изображая чрезъ c число, удовлетворяющее условію

$$\left(\frac{D}{c}\right) = -1,$$

возьмемъ во вниманіе произведеніе cx и обозначимъ его наименьшій положительный вычетъ по модулю $4D$ чрезъ y.

Если x, послѣдовательно измѣняясь, перейдетъ чрезъ всѣ $\varphi(4D)$ значеній простыхъ относительно $4D$ и меньше числовой величины $4D$, въ то время y, соотвѣтственно измѣняясь, перейдетъ чрезъ тѣ же самыя значенія. Отсюда вытекаетъ уравненіе

$$\sum\left(\frac{D}{x}\right) = \sum\left(\frac{D}{y}\right),$$

гдѣ знаки суммы простираются на всѣ вышеупомянутыя значенія перемѣннаго x и на всѣ соотвѣтствующія имъ значенія y. Съ другой стороны, такъ какъ $cx \equiv y$ (mod. $4D$), то

$$\left(\frac{D}{y}\right) = \left(\frac{D}{cx}\right).$$

Изъ послѣднихъ двухъ уравненій выводимъ

$$\sum\left(\frac{D}{x}\right) = \sum\left(\frac{D}{cx}\right).$$

А такъ какъ

$$\left(\frac{D}{cx}\right) = \left(\frac{D}{c}\right)\left(\frac{D}{x}\right) = -\left(\frac{D}{x}\right),$$

то слѣдовательно

$$\sum\left(\frac{D}{x}\right) = -\sum\left(\frac{D}{x}\right);$$

откуда заключаемъ

(1) . . . . $\sum\left(\frac{D}{x}\right) = 0.$

Если обозначимъ чрезъ m число членовъ равныхъ 1 въ первой части послѣдняго уравненія, а чрезъ m' число членовъ равныхъ -1, то уравненіе (1) можно написать такъ:

$$m - m' = 0;$$

при этомъ имѣемъ очевидно

$$m + m' = \varphi(4D);$$

слѣдовательно

$$m = m' = \tfrac{1}{2}\varphi(4D),$$

что и требовалось доказать.

Теорема 2. *Если* $D \equiv 1 \pmod{4}$, *то между числами, простыми относительно* $2D$ *и не превышающими числовой величины* $2D$, *половина удовлетворяетъ уравненію*

$$\left(\frac{D}{x}\right) = 1,$$

другая половина — уравненію

$$\left(\frac{D}{x}\right) = -1.$$

Теорему эту легко доказать такимъ же образомъ, какъ и предыдущую, но можно также вывести ее, какъ слѣдствіе предыдущей. Дѣйствительно, обозначивъ чрезъ Δ числовую величину D, мы замѣчаемъ, что въ то время, когда перемѣнное x будетъ принимать послѣдовательно всѣ значенія, простыя съ $2D$ и меньше 2Δ, сумма $x + 2\Delta$ перейдетъ чрезъ всѣ значенія, простыя съ $2D$ и содержащіяся въ промежуткѣ отъ 2Δ до 4Δ. Поэтому уравненіе (1) можно написать такъ:

$$\sum\left(\frac{D}{x}\right) + \sum\left(\frac{D}{x + 2\Delta}\right) = 0,$$

причемъ знакъ суммы простирается на всѣ $\varphi(2D)$ значеній x, простыхъ относительно $2D$ и меньше 2Δ.

Но по одной изъ вышедоказанныхъ теоремъ имѣемъ

$$\left(\frac{D}{x+2\Delta}\right)=\left(\frac{D}{x}\right);$$

слѣдовательно

$$2\sum\left(\frac{D}{x}\right)=0,$$

или

$$\sum\left(\frac{D}{x}\right)=0,$$

гдѣ знакъ суммы простирается на значенія x меньше числовой величины $2D$. Отсюда заключаемъ непосредственно о справедливости предложенной нами теоремы.

Примѣры. Полагая послѣдовательно $D=2, 3, 5, 6, \ldots$ или $D=-1, -2, -3, \ldots$ находимъ нижеслѣдующія рѣшенія для уравненій вида

$$\left(\frac{D}{x}\right)=1.$$

D	x
2	1, 7.
3	1, 11.
5	1, 9, 11, 19.
6	1, 5, 19, 23.
7	1, 3, 9, 19, 25, 27.
10	1, 3, 9, 13, 27, 31, 37, 39.
11	1, 5, 7, 9, 19, 25, 35, 37, 39, 43.
13	1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51.
14	1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55.
15	1, 7, 11, 17, 43, 49, 53, 59.
17	1, 9, 13, 15, 19, 21, 25, 33, 35, 43, 47, 49, 53, 55, 59, 67.
19	1, 3, 5, 9, 15, 17, 25, 27, 31, 45, 49, 51, 59, 61, 67, 71, 73, 75.
. . .	. . . .

D	x
— 1	1.
— 2	1, 3.
— 3	1, 7.
— 5	1, 3, 7, 9.
— 6	1, 5, 7, 11.
— 7	1, 9, 11, 15, 23, 25.
—10	1, 7, 9, 11, 13, 19, 23, 37.
—11	1, 3, 5, 9, 15, 23, 25, 27, 31, 37.
—13	1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49.
—14	1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45.
—15	1, 17, 19, 23, 31, 47, 49, 53.
—17	1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63.
—19	1,5,7,9,11,17,23,25,35,39,43,45,47,49,55,61,63,73.
. . .	. . . .

Здѣсь выписаны только тѣ рѣшенія, которыя меньше числовой величины $4D$; каждое изъ нихъ опредѣляетъ собой безконечное множество чиселъ, удовлетворяющихъ уравненію $\left(\frac{D}{x}\right) = 1$. Такъ, напримѣръ, всѣ рѣшенія уравненія

$$\left(\frac{6}{x}\right) = 1$$

опредѣляются по формуламъ

$$x \equiv 1 \text{ (mod. 24)}, \quad x \equiv 5 \text{ (mod. 24)},$$
$$x \equiv 19 \text{ (mod. 24)}, \quad x \equiv 23 \text{ (mod. 24)}.$$

Въ случаѣ, когда $D \equiv 1$ (mod. 4), довольно знать половину выписанныхъ нами рѣшеній, именно тѣ, которыя меньше числовой величины $2D$; ибо съ ними сравнимы по модулю $2D$ всѣ остальныя рѣшенія уравненія $\left(\frac{D}{x}\right) = 1$. Напримѣръ, всѣ рѣшенія уравненія

$$\left(\frac{-7}{x}\right) = 1$$

опредѣляются по слѣдующимъ тремъ формуламъ:

$$x \equiv 1 \pmod{14}, \quad x \equiv 9 \pmod{14}, \quad x \equiv 11 \pmod{14}.$$

62. Вопросъ объ отысканіи дѣлителей даннаго числа есть одинъ изъ основныхъ и самыхъ важныхъ въ теоріи чиселъ; имъ занимались такіе математики, какъ Эйлеръ и Гауссъ. Способы, предложенные ими, оставляютъ желать многаго, тѣмъ не менѣе они даютъ возможность очень часто преодолѣвать трудности сравнительно легко; пока, само собою разумѣется, данное число не слишкомъ большое.

Не находя возможнымъ вдаваться здѣсь въ подробности относительно этого предмета, мы ограничимся нѣсколькими общими замѣчаніями.

Наименьшій дѣлитель сложнаго числа a, послѣ единицы, есть всегда нѣкоторое простое число, не превышающее $\sqrt{a}$. Для опредѣленія его приходится испытывать поочередно всѣ цѣлыя числа, не превышающія $\sqrt{a}$; и если между ними не найдется ни одного, который бы дѣлилъ a, то a будетъ числомъ простымъ. Понятно, что такое испытываніе при значительномъ a представляется невыполнимымъ; тогда необходимо искать особыхъ указаній, вытекающихъ изъ индивидуальныхъ свойствъ заданнаго числа, которыя дали бы возможность уменьшить въ достаточной степени число чиселъ подлежащихъ испытанію.

Всякое число можетъ быть представлено въ видѣ квадратичнаго двучлена

$$(1) \ldots\ldots\ldots\ldots\ldots a = t^2 - Du^2,$$

гдѣ t, u, D цѣлыя числа отличныя отъ нуля, и очевидно, что такое представленіе можетъ быть выполнено безчисленными способами. Допустивъ, что заданное число a уже представлено въ видѣ (1), мы замѣчаемъ, что въ случаѣ, когда t и Du имѣютъ общій дѣлитель, разложеніе a на произведеніе двухъ множителей получается непосредственно; поэтому мы предположимъ, что t простое съ Du. Тогда имѣетъ мѣсто слѣдующая теорема.

Теорема. *Всякій нечетный дѣлитель формы $t^2 - Du^2$ удовлетворяетъ уравненію*

$$\left(\frac{D}{x}\right) = 1.$$

Очевидно, что достаточно доказать справедливость теоремы для простаго дѣлителя числа $t^2 - Du^2$. Обозначивъ чрезъ p одинъ изъ такихъ дѣлителей, имѣемъ

$$t^2 - Du^2 \equiv 0 \pmod{p}.$$

Здѣсь u не дѣлится на p; ибо въ противномъ случаѣ t дѣлилось бы на p, а между тѣмъ t простое съ u. Слѣдовательно можно найти число u', удовлетворяющее условію

$$uu' \equiv 1 \pmod{p}.$$

Умножая обѣ части предшествующаго сравненія на u'^2, получаемъ

$$(tu')^2 - D(uu')^2 \equiv 0 \pmod{p},$$

откуда заключаемъ

$$(tu')^2 - D \equiv 0 \pmod{p}.$$

Но D не дѣлится на p; ибо въ противномъ случаѣ t дѣлилось бы на p, между тѣмъ D простое съ t; слѣдовательно имѣемъ

$$\left(\frac{D}{p}\right) = 1,$$

что и слѣдовало доказать.

Слѣдствіе. *Всякій нечетный дѣлитель суммы двухъ взаимно простыхъ квадратовъ есть вида* $4n + 1$.

Въ самомъ дѣлѣ, такой дѣлитель долженъ удовлетворять уравненію $\left(\frac{-1}{x}\right) = 0$, которое по модулю 4 имѣетъ одно только рѣшеніе $x = 1$.

Слѣдствіе это вытекаетъ также непосредственно изъ леммы n^0 35.

Если намъ удастся данное число a или какія нибудь его кратности представить нѣсколькими способами въ видѣ квадратичныхъ формъ

$$la = t^2 - Du^2,$$

$$l'a = t'^2 - D'u'^2,$$

$$\dots\dots\dots\dots$$

$$l''a = t''^2 - D''u''^2,$$

гдѣ Du, $D'u'$,... суть числа простыя относительно a, то тогда всякій дѣлитель числа a долженъ будетъ удовлетворять каждому изъ уравненій

$$(2) \dots\dots\dots \left(\frac{D}{x}\right) = 1, \left(\frac{D'}{x}\right) = 1, \dots \left(\frac{D''}{x}\right) = 1.$$

При небольшихъ значеніяхъ D, D',... можно воспользоваться таблицами рѣшеній уравненій вида (2). По нимъ легко вычислить рѣшенія, общія всѣмъ уравненіямъ (2) и не превышающія $\sqrt{a}$. Въ числѣ этихъ послѣднихъ слѣдуетъ искать наименьшаго дѣлителя числа a.

ГЛАВА VI.

Сравненіе второй степени при сложномъ модулѣ.

§ 1. Случай, когда модуль есть степень простаго числа.

63. Всякое число, удовлетворяющее сравненію

$$(1) \ldots\ldots\ldots\ldots f(x) \equiv 0 \pmod{p^m},$$

удовлетворяетъ очевидно и сравненію

$$(2) \ldots\ldots\ldots\ldots f(x) \equiv 0 \pmod{p^{m-1}};$$

поэтому корни (1) слѣдуетъ отыскивать между корнями (2). Если сравненіе (2) невозможно, то и (1) также невозможно.

Обозначивъ чрезъ a любой корень (2), мы имѣемъ формулу

$$x = a + p^{m-1}t,$$

опредѣляющую безчисленное множество чиселъ, принадлежащихъ вмѣстѣ съ a къ одному и тому же классу по модулю p^{m-1}; посмотримъ, нѣтъ ли между ними такихъ, которыя удовлетворяли бы сравненію (1). Для этого составляемъ сравненіе

$$f(a + p^{m-1}t) \equiv 0 \pmod{p^m},$$

которое можно написать такъ:

$$f(a)+p^{m-1}tf'(a)+p^{2m-2}t^2f''(a)+\ldots\equiv 0 \pmod{p^m},$$

или, проще,

$$f(a)+p^{m-1}tf'(a)\equiv 0 \pmod{p^m};$$

ибо $m\geqq 2$, вслѣдствіе чего имѣемъ $2m-2\geqq m$.

Но число $f(a)$ дѣлится на p^{m-1}; поэтому послѣднее сравненіе можно сократить на p^{m-1} и представить въ болѣе простомъ видѣ, именно,

(3) . . . . $f'(a)t+b\equiv 0 \pmod{p}$,

гдѣ b изображаетъ частное, полученное отъ дѣленія $f(a)$ на p^{m-1}.

Сравненіе (3) — первой степени; если оно невозможно, то сравненіе (1) не имѣетъ ни одного корня сравнимаго съ a по модулю p^{m-1}.

Такимъ образомъ всѣ корни сравненія (1) образуютъ нѣсколько группъ, которыя опредѣляются различными корнями (2); вычисленіе корней, принадлежащихъ къ опредѣленной группѣ a, состоитъ въ рѣшеніи нѣкотораго сравненія первой степени съ модулемъ p.

Примѣняя предыдущія разсужденія къ сравненію (2), мы заключаемъ, что опредѣленіе его корней приводится въ свою очередь къ рѣшенію сравненія

$$f(x)\equiv 0 \pmod{p^{m-2}}$$

и затѣмъ еще къ рѣшенію нѣкотораго сравненія первой степени съ модулемъ p.

Продолжая далѣе подобное разсужденіе, мы замѣчаемъ, что рѣшеніе сравненія (1) всегда можно свести на рѣшеніе сравненія

$$f(x)\equiv 0 \pmod{p}$$

и еще $p-1$ отдѣльныхъ сравненій первой степени, каждое съ модулемъ p.

Послѣднее предложеніе имѣетъ мѣсто независимо отъ того, будетъ ли число p простымъ или сложнымъ; но чаще всего приходится предполагать p простымъ, ибо уже раньше было доказано, что рѣшеніе всякаго сравненія со сложнымъ модулемъ приводится къ рѣшенію нѣсколькихъ сравненій, модули которыхъ суть степени простыхъ чиселъ.

64. Особеннаго изслѣдованія заслуживаетъ сравненіе двучленное

$$(1) \quad \ldots\ldots\ldots\ldots \quad x^2 \equiv q \ (\mathrm{mod.}\ p^m);$$

на немъ мы желаемъ теперь остановиться.

Допустимъ сперва, что простое число p больше 2. Тогда легко составить окончательное правило, дающее возможность, по данному рѣшенію сравненія

$$(2) \quad \ldots\ldots\ldots\ldots \quad x^2 \equiv q \ (\mathrm{mod.}\ p),$$

вычислить рѣшеніе (1).

Изображая чрезъ a число удовлетворяющее (2), возьмемъ во вниманіе степень $(a+\sqrt{q})^m$ и представимъ ее такъ:

$$(3) \quad \ldots\ldots\ldots\ldots \quad (a+\sqrt{q})^m = P + Q\sqrt{q},$$

гдѣ P и Q изображаютъ цѣлыя числа,

$$P = a^m + \frac{m(m-1)}{1.2} a^{m-2} q + \ldots,$$

$$Q = \frac{m}{1} a^{m-1} + \frac{m(m-1)(m-2)}{1.2.3} a^{m-3} q + \ldots$$

Одновременно съ (3) имѣетъ мѣсто равенство

$$(4) \quad \ldots\ldots\ldots\ldots \quad (a-\sqrt{q})^m = P - Q\sqrt{q}.$$

Перемножая (3) и (4) между собой, получаемъ

$$(a^2-q)^m = P^2 - Q^2 q;$$

а такъ какъ по предположенію $a^2 - q \equiv 0 \pmod{p}$, то слѣдовательно

$$(5) \ldots\ldots\ldots\ldots P^2 - Q^2 q \equiv 0 \pmod{p^m}.$$

Съ другой стороны, какова бы ни была цѣлая функція $f(x)$, имѣемъ

$$f(q) \equiv f(a^2) \pmod{p}.$$

Полагая здѣсь

$$f(x) = \frac{(a+\sqrt{x})^m - (a-\sqrt{x})^m}{2\sqrt{x}} = \frac{m}{1} a^{m-1} + \frac{m(m-1)(m-2)}{1.2.3} a^{m-3} x + \ldots,$$

получаемъ

$$Q \equiv 2^{m-1} a^{m-1} \pmod{p}.$$

Отсюда легко заключить, что Q не дѣлится на p. Ибо въ противномъ случаѣ число a должно было бы дѣлиться на p; но такъ какъ $a^2 \equiv q \pmod{p}$, то слѣдовательно и q дѣлилось бы на p, что, конечно, не предполагается.

Такъ какъ Q не дѣлится на p, то сравненіе

$$Qx \equiv P \pmod{p^m}$$

возможно. Обозначивъ чрезъ x какое либо изъ его рѣшеній, имѣемъ

$$(6) \ldots\ldots\ldots\ldots Q^2 x^2 \equiv P^2 \pmod{p^m}.$$

Изъ (5) и (6) выводимъ

$$Q^2 x^2 \equiv Q^2 q \pmod{p^m},$$

откуда, сокращая на Q^2, получаемъ

$$x^2 \equiv q \pmod{p^m}.$$

Это показываетъ, что рѣшеніе сравненія первой степени

$$Qx \equiv P \pmod{p^m}$$

будетъ корнемъ сравненія (1).

Найдя такимъ образомъ одинъ корень сравненія (1), мы найдемъ сейчасъ и другой его корень, перемѣняя только знакъ у x.

Обозначивъ теперь чрезъ y какое нибудь изъ чиселъ, удовлетворяющихъ (1), имѣемъ два сравненія

$$y^2 \equiv q \pmod{p^m}, \quad x^2 \equiv q \pmod{p^m},$$

изъ которыхъ выводимъ

$$y^2 - x^2 \equiv 0 \pmod{p^m},$$

или

$$(y - x)(y + x) \equiv 0 \pmod{p^m}.$$

Одинъ изъ множителей въ первой части есть простой относительно p; ибо въ противномъ случаѣ мы имѣли бы два сравненія

$$\left.\begin{aligned} y - x &\equiv 0 \\ y + x &\equiv 0 \end{aligned}\right\} \pmod{p};$$

отсюда

$$2x \equiv 0 \pmod{p},$$

что очевидно невозможно. Слѣдовательно имѣетъ мѣсто одно изъ двухъ:

$$y - x \equiv 0 \pmod{p^m}$$

или

$$y + x \equiv 0 \pmod{p^m};$$

въ первомъ случаѣ имѣемъ $y \equiv x \pmod{p^m}$, во второмъ $y \equiv -x \pmod{p^m}$. Это показываетъ, что другихъ корней, кромѣ двухъ вышенайденныхъ, сравненіе (1) не имѣетъ.

Такъ мы убѣдились въ справедливости слѣдующей теоремы.

Теорема. *Если p число простое нечетное, а q не дѣлится на p, то сравненіе*

$$x^2 \equiv q \pmod{p^m}$$

или невозможно, или имѣетъ два рѣшенія; первый случай имѣетъ мѣсто, если $\left(\frac{q}{p}\right) = -1$; *второй, если* $\left(\frac{q}{p}\right) = 1$.

65. Переходимъ теперь къ рѣшенію сравненія

(1) . . . . $x^2 \equiv q \pmod{2^m}$,

предполагая, конечно, что q число нечетное.

Будемъ разсматривать отдѣльно четыре случая:

Первый случай, $m = 1$. Тогда сравненіе (1) можно написать такъ:

$$x^2 \equiv 1 \pmod{2},$$

и очевидно, что оно имѣетъ одно только рѣшеніе

$$x \equiv 1 \pmod{2}.$$

Второй случай, $m = 2$. Тогда имѣемъ сравненіе

$$x^2 \equiv q \pmod{4},$$

которое можно написать въ одномъ изъ двухъ видовъ:

(2) . . . . $x^2 \equiv 1 \pmod{4}$

или

(3) . . . . $x^2 \equiv -1 \pmod{4}$,

смотря по тому будетъ ли число q вида $4n + 1$ или вида $4n - 1$.

Сравненіе (2) имѣетъ очевидно два рѣшенія, именно:

$$x \equiv 1 \pmod{4} \quad \text{и} \quad x \equiv 3 \pmod{4};$$

сравненіе (3) невозможно.

Третій случай, $m = 3$. Имѣемъ

(4) . . . . $x^2 \equiv q \pmod{8}$.

Неизвѣстное x должно быть числомъ нечетнымъ; но легко убѣдиться, что квадратъ всякаго нечетнаго числа сравнимъ съ 1 по модулю 8:

$$(4n \pm 1)^2 = 1 + 8(2n^2 \pm n) \equiv 1 \pmod{8};$$

слѣдовательно сравненіе (4) возможно только при условіи

$$q \equiv 1 \ (\text{mod. } 8).$$

Если оно выполнено, то сравненіе (4) представляется въ видѣ

$$x^2 \equiv 1 \ (\text{mod. } 8),$$

и всякое нечетное число удовлетворяетъ ему; число корней равно 4.

Четвертый случай, $m > 3$. Тогда легко показать, что сравненіе (1) или не имѣетъ вовсе рѣшеній, или имѣетъ ихъ четыре.

Допустимъ сперва, что сравненіе

$$x^2 \equiv q \ (\text{mod. } 2^m)$$

имѣетъ рѣшеніе, и пусть x изображаетъ какое либо число, удовлетворяющее ему. Если y есть число отличное отъ x, но удовлетворяющее тому же сравненію, то

$$y^2 \equiv x^2 \ (\text{mod. } 2^m),$$

или

$$(y - x)(y + x) \equiv 0 \ (\text{mod. } 2^m).$$

Оба множителя въ первой части суть четные; раздѣляя обѣ части сравненія и модуль на 4, получаемъ

$$\frac{y-x}{2} \, \frac{y+x}{2} \equiv 0 \ (\text{mod. } 2^{m-2}).$$

Теперь множители въ первой части не могутъ быть оба четными, ибо ихъ сумма есть нечетная; поэтому заключаемъ, что непремѣнно должно имѣть мѣсто одно изъ двухъ сравненій:

$$\frac{y-x}{2} \equiv 0 \ (\text{mod. } 2^{m-2})$$

или

$$\frac{y+x}{2} \equiv 0 \ (\text{mod. } 2^{m-2}).$$

Другими словами, будемъ имѣть одно изъ двухъ:

$$y = x + 2^{m-1}t$$

или

$$y = -x + 2^{m-1}t,$$

гдѣ t изображаетъ цѣлое число, которое можетъ быть или четнымъ или нечетнымъ.

Подставляя въ послѣднихъ двухъ формулахъ на мѣсто t сперва $2t$, а послѣ $2t + 1$, получаемъ для числа y четыре слѣдующихъ вида:

$$y = x + 2^m t,$$
$$y = x + 2^{m-1} + 2^m t,$$
$$y = -x + 2^m t,$$
$$y = -x + 2^{m-1} + 2^m t,$$

что можно представить проще такъ:

$$\left.\begin{aligned} y &\equiv x \\ y &\equiv x + 2^{m-1} \\ y &\equiv -x \\ y &\equiv -x + 2^{m-1} \end{aligned}\right\} (\text{mod. } 2^m).$$

Отсюда ясно, что кромѣ рѣшенія x сравненіе (1) можетъ имѣть еще только три рѣшенія; и на самомъ дѣлѣ оно ихъ всегда будетъ имѣть; ибо числа

$$x,\ x + 2^{m-1},\ -x,\ -x + 2^{m-1}$$

очевидно несравнимы между собою по модулю 2^m, и каждое изъ нихъ удовлетворяетъ сравненію (1).

Докажемъ теперь, что если сравненіе

(5) . . . . $x^2 \equiv q \ (\text{mod. } 2^{m-1})$

возможно, то между его четырьмя рѣшеніями найдется два и только два, которыя будутъ удовлетворять сравненію

$$(6) \ldots\ldots\ldots\ldots x^2 \equiv q \pmod{2^m}.$$

На самомъ дѣлѣ, обозначивъ чрезъ a любой корень сравненія (5), всѣ четыре корня того же сравненія можно выразить такъ:

$$a, \quad -a, \quad a+2^{m-2}, \quad -a+2^{m-2}.$$

Отсюда видно, что если одинъ изъ корней сравненія (5), напримѣръ a, удовлетворяетъ (6), то тому же сравненію будетъ удовлетворять и другой корень (5), именно $-a$. Что касается остальныхъ двухъ корней сравненія (5), то изъ нихъ ни одинъ не будетъ удовлетворять (6). Ибо вторая часть равенства

$$(2^{m-2} \pm a)^2 - q = a^2 - q + 2^{m-1}(2^{m-3} \pm a)$$

при $m > 3$ очевидно не дѣлится на 2^m.

Напротивъ, если a не удовлетворяетъ (6), то и $-a$ не удовлетворяетъ ему; тогда частное

$$\frac{a^2-q}{2^{m-1}}$$

будетъ числомъ нечетнымъ, и вторая часть равенства

$$(2^{m-2} \pm a)^2 - q = 2^{m-1}\left[\frac{a^2-q}{2^{m-1}} + 2^{m-3} \pm a\right]$$

будетъ очевидно дѣлиться на 2^m. Слѣдовательно послѣдніе два корня (5) будутъ также корнями (6).

Переходя теперь къ выводу условія, при которомъ сравненіе

$$x^2 \equiv q \pmod{2^m}, \quad (m > 3),$$

возможно, мы замѣчаемъ, что возможность означеннаго сравненія влечетъ за собою возможность сравненія

$$x^2 \equiv q \pmod{8},$$

что въ свою очередь приводитъ къ сравненію

(7) . . . . $q \equiv 1 \pmod{8}$.

Наоборотъ, если условіе (7) удовлетворено, то сравненіе

$$x^2 \equiv q \pmod{2^m}$$

возможно.

Чтобы убѣдиться въ этомъ, мы будемъ разсуждать такъ:

На основаніи (7) заключаемъ, что сравненіе

$$x^2 \equiv q \pmod{8}$$

имѣетъ рѣшенія. По вышедоказанному, изъ числа четырехъ его корней два будутъ удовлетворять сравненію

$$x^2 \equiv q \pmod{2^4}.$$

Поэтому послѣднее сравненіе будетъ имѣть четыре корня, изъ коихъ два будутъ удовлетворять сравненію

$$x^2 \equiv q \pmod{2^5}.$$

Это сравненіе въ свою очередь будетъ имѣть четыре корня, изъ коихъ два будутъ удовлетворять сравненію

$$x^2 \equiv q \pmod{2^6}.$$

Разсуждая такимъ образомъ все далѣе и далѣе, мы приходимъ къ заключенію, что, каково бы ни было цѣлое число $m > 3$, сравненіе

$$x^2 \equiv q \pmod{2^m}$$

будетъ имѣть четыре рѣшенія; такъ что условіе (7) оказывается не только необходимымъ, но и достаточнымъ.

Резюмируя полученные результаты, мы приходимъ къ слѣдующей теоремѣ.

Теорема. *Сравненіе*

$$x^2 \equiv q \pmod{2^m}$$

при нечетномъ q представляетъ слѣдующіе случаи:

1° *если $m = 1$, оно имѣетъ одинъ корень;*

2° *если $m = 2$, оно имѣетъ два корня или ни одного, смотря по тому, будетъ ли удовлетворено условіе $q \equiv 1 \pmod{4}$ или не будетъ;*

3° *если $m \geq 3$, сравненіе имѣетъ четыре корня или ни одного, смотря по тому, будетъ ли удовлетворено условіе $q \equiv 1 \pmod{8}$ или не будетъ.*

Въ послѣднемъ случаѣ, если условіе $q \equiv 1 \pmod{8}$ удовлетворено, два корня сравненія

$$x^2 \equiv q \pmod{2^m}$$

удовлетворяютъ также и сравненію

$$x^2 \equiv q \pmod{2^{m+1}};$$

остальные два этимъ свойствомъ не обладаютъ.

Примѣръ. Требуется найти корни сравненія

$$x^2 \equiv 17 \pmod{2^7}.$$

Начинаемъ со сравненія

$$x^2 \equiv 17 \pmod{8},$$

которое можно написать такъ:

$$x^2 \equiv 1 \pmod{16}.$$

Отсюда прямо опредѣляемъ четыре корня

$$\pm 1, \quad \pm 7.$$

Переходимъ къ сравненію

$$x^2 \equiv 17 \pmod{32};$$

четыре его корня суть слѣдующіе:

$$\pm 7, \ \pm 9.$$

Переходимъ далѣе къ сравненію

$$x^2 \equiv 17 \ (\text{mod. } 64),$$

и находимъ его корни:

$$\pm 9, \ \pm 23.$$

Переходя наконецъ къ сравненію

$$x^2 \equiv 17 \ (\text{mod. } 128),$$

находимъ его корни:

$$\pm 23, \ \pm 41.$$

§ II. Число рѣшеній сравненія $x^2 \equiv q$ (mod. k) при сложномъ модулѣ. Слѣдствія.

66. Теперь не трудно вывести условія достаточныя и необходимыя для того, чтобы сравненіе

$$(1) \ldots\ldots\ldots\ldots\ldots x^2 \equiv q \ (\text{mod. } k)$$

при сложномъ k было возможно, предполагая притомъ, что q простое съ k; въ случаѣ возможности (1) легко также опредѣлить число корней. Для этого мы принимаемъ во вниманіе разложеніе модуля на простые множители

$$k = 2^m p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n},$$

гдѣ m можетъ равняться нулю, и замѣчаемъ, что опредѣленіе корней сравненія (1) приводится къ вычисленію корней каждаго изъ слѣдующихъ сравненій:

$$(2) \ldots\ldots\ldots\ldots \begin{cases} x^2 \equiv q \pmod{2^m}, \\ x^2 \equiv q \pmod{p_1^{m_1}}, \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ x^2 \equiv q \pmod{p_n^{m_n}}. \end{cases}$$

Но чтобы каждое изъ нихъ было возможно, для этого необходимы такія условія:

$$q \equiv 1 \text{ (mod. 4), если } m = 2;$$

$$q \equiv 1 \text{ (mod. 8), если } m > 2;$$

$$\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right) = \ldots = \left(\frac{q}{p_n}\right) = 1.$$

Если они выполнены, то число рѣшеній перваго сравненія (2) равно

$$2^\sigma,$$

гдѣ $\sigma = 0$, 1 или 2, смотря по тому будетъ ли $m < 2$, $m = 2$ или $m > 2$; что касается остальныхъ сравненій (2), то каждое изъ нихъ будетъ имѣть по два рѣшенія. Слѣдовательно по теоремѣ n^0 42 число всѣхъ корней сравненія (1) равно

$$2^{\sigma+n}.$$

67. Обозначивъ, какъ въ предыдущемъ номерѣ, чрезъ k какое нибудь сложное число

$$k = 2^m p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n},$$

а чрезъ q какое угодно число, простое съ k, мы возьмемъ во вниманіе рядъ

$$(1) \ldots\ldots\ldots\ldots 1, a, b, \ldots k-1,$$

состоящій изъ всѣхъ чиселъ $< k$ и простыхъ съ k. Каждому изъ этихъ чиселъ, напримѣръ a, соотвѣтствуетъ нѣкоторое

Итакъ, во всякомъ частномъ случаѣ имѣетъ мѣсто (2) или (3), смотря по тому, будетъ ли q квадратичнымъ невычетомъ или вычетомъ числа k. Изъ (3) выводимъ, дѣлая $q = 1$,

$$(4) \ldots\ldots 1.\, a \ldots (k-1) \equiv (-1)^{2^{n+\sigma-1}} \pmod{k},$$

что приводитъ къ слѣдующей теоремѣ Гаусса.

Теорема 1. *Обозначимъ для сокращенія чрезъ* Π *произведеніе всѣхъ чиселъ* $< k$ *и простыхъ съ* k.

Если k *есть степень простаго нечетнаго числа, или удвоенная степень простаго нечетнаго числа, или* $k = 2$, *или* $k = 4$, — *во всѣхъ этихъ случаяхъ имѣемъ*

$$\Pi \equiv -1 \pmod{k}.$$

Въ остальныхъ случаяхъ, напротивъ,

$$\Pi \equiv 1 \pmod{k}.$$

Теорема эта представляетъ очевидно обобщеніе извѣстной теоремы Вильсона.

Принимая во вниманіе (4), изъ (2) и (3) выводимъ

$$q^{\frac{1}{2}\varphi(k)} \equiv (-1)^{2^{n+\sigma-1}} \pmod{k},$$

$$q^{\frac{1}{2}\varphi(k)} \equiv 1 \pmod{k}.$$

Первое изъ этихъ сравненій требуетъ, чтобы q было квадратичнымъ невычетомъ числа k, второе, напротивъ, требуетъ, чтобы q было квадратичнымъ вычетомъ относительно k. Оба они совпадаютъ между собой, если $n + \sigma > 1$; напротивъ, они существенно различны, если $n + \sigma = 1$. Это приводитъ къ такой теоремѣ.

Теорема 2. *Если* k *есть степень простаго нечетнаго числа, или удвоенная степень простаго нечетнаго числа, или* $k = 4$, — *во всѣхъ этихъ случаяхъ имѣемъ одно изъ двухъ:*

$$q^{\frac{1}{2}\varphi(k)} \equiv 1 \pmod{k}$$

или

$$q^{\frac{1}{2}\varphi(k)} \equiv -1 \pmod{k},$$

смотря по тому будетъ ли q квадратичнымъ вычетомъ или невычетомъ числа k.

Въ остальныхъ случаяхъ, каково бы ни было число q, всегда имѣемъ

$$q^{\frac{1}{2}\varphi(k)} \equiv 1 \pmod{k}.$$

Отсюда, какъ прямое слѣдствіе, получается сравненіе

$$q^{\varphi(k)} \equiv 1 \pmod{k}$$

для всякаго k и всякаго q простаго съ k. Это извѣстная теорема Эйлера.

ГЛАВА VII.

О сравненіяхъ высшихъ степеней. — Двучленныя сравненія.

§ I. Теорема Лагранжа.

68. Въ предшествующихъ главахъ (n^0 42, 63) было показано, какимъ образомъ рѣшеніе сравненія со сложнымъ модулемъ приводится къ рѣшенію нѣсколькихъ сравненій, каждое съ простымъ модулемъ. Къ этому слѣдуетъ прибавить, что важнѣйшіе и самые любопытные результаты, добытые въ теоріи сравненій, относятся къ случаю, когда модуль простой. Вотъ почему въ дальнѣйшемъ изложеніи мы ограничимся простымъ модулемъ, и каждый разъ, когда придется дѣлать отступленіе отъ этого предположенія, мы будемъ оговариваться.

Теорема. *Число корней сравненія не превышаетъ его степени.*

Для сравненій первыхъ двухъ степеней справедливость теоремы вытекаетъ прямо изъ того, что было доказано въ предыдущихъ главахъ.

Допустивъ, что теорема справедлива для всякаго сравненія ($n-1$)-ой степени, мы покажемъ, что она справедлива и для всякаго сравненія n-ой степени; очевидно, что такимъ образомъ справедливость теоремы будетъ доказана вполнѣ. Такъ какъ для

невозможнаго сравненія справедливость теоремы очевидна, то можно ограничиться предположеніемъ, что сравненіе

(1). . . . . $Ax^n + A_1x^{n-1} + \ldots + A_n \equiv 0 \pmod{p}$

возможно.

Обозначивъ чрезъ a какой либо изъ его корней, раздѣлимъ функцію

$$f(x) = Ax^n + A_1x^{n-1} + \ldots + A_n,$$

на $x - a$. Изображая частное чрезъ $\varphi(x)$, имѣемъ тожество

$$f(x) = (x - a)\,\varphi(x) + f(a),$$

вслѣдствіе чего сравненіе (1) можно написать такъ:

(2) . . . . $(x - a)\,\varphi(x) + f(a) \equiv 0 \pmod{p}$.

Но по предположенію имѣемъ

$$f(a) \equiv 0 \pmod{p};$$

поэтому сравненіе (2) равносильно слѣдующему:

(3). . . . . $(x - a)\,\varphi(x) \equiv 0 \pmod{p}$.

Всякое значеніе x, удовлетворяющее (3) и не сравнимое съ a по модулю p, должно удовлетворять сравненію

(4) . . . . $\varphi(x) \equiv 0 \pmod{p}$;

слѣдовательно всѣ корни сравненія (1), отличные отъ a, будутъ корнями сравненія (4). Но послѣднее сравненіе, будучи степени $(n-1)$-ой, не можетъ, по предположенію, имѣть болѣе $n-1$ корней; слѣдовательно сравненіе (1) не можетъ имѣть болѣе $n-1$ корней отличныхъ отъ a, а потому число всѣхъ его корней вмѣстѣ съ a не можетъ превышать n. Что и слѣдовало доказать.

Слѣдствіе. *Если сравненіе*

$$Ax^n + A_1x^{n-1} + \ldots + A_n \equiv 0 \ (\text{mod.}\, p)$$

по виду n-ой степени имѣетъ болѣе n корней, то всѣ коэффиціенты A, A_1, . . . A_n дѣлятся на p.

Въ противномъ случаѣ мы имѣли бы сравненіе степени *не выше n*, которое имѣло бы болѣе n корней, что невозможно.

Такъ, напримѣръ, сравненіе

$$(5) \quad x^{p-1} - 1 - (x-1)(x-2)\ldots(x-p+1) \equiv 0 \ (\text{mod.}\, p)$$

по виду есть $(p-2)$-ой степени; между тѣмъ ясно, если принять во вниманіе теорему Фермата, что всѣ числа отъ 1 до $p-1$ удовлетворяютъ ему. Поэтому коэффиціенты у различныхъ степеней x въ первой части (5) дѣлятся на p, и мы можемъ написать

$$x^{p-1} - 1 = (x-1)(x-2)\ldots(x-p+1) + pF(x),$$

гдѣ $F(x)$ изображаетъ цѣлую функцію съ цѣлыми коэффиціентами. Такимъ образомъ съ помощью теоремы Лагранжа получается прямо равенство, доказанное нами на страницѣ 88. Полагая въ немъ $x=0$, получаемъ теорему Вильсона.

При сложномъ модулѣ теорема Лагранжа иногда имѣетъ мѣсто, иногда не имѣетъ; это видно уже для сравненій первыхъ двухъ степеней.

Перейдемъ теперь къ изложенію новаго начала, весьма важнаго въ общей теоріи сравненій, которое приведетъ насъ вновь къ теоремѣ Лагранжа.

§ II. Разложеніе функцій на множители по данному модулю. О функціяхъ неприводимыхъ по данному модулю.

69. Двѣ функціи съ цѣлыми коэффиціентами

$$f(x) = a + a_1x + \ldots + a_nx^n,$$

$$f_1(x) = b + b_1x + \ldots + b_nx^n$$

называются ***сравнимыми по модулю*** p, если соотвѣтствующіе коэффиціенты въ ихъ выраженіяхъ сравнимы, то есть,

$$a \equiv b, \ a_1 \equiv b_1, \ldots a_n \equiv b_n \pmod{p}.$$

Тогда пишутъ

$$(x) \equiv f_1(x) \pmod{p},$$

и сравненіе такое называютъ *тожественнымъ*.

Если всѣ коэффиціенты въ выраженіи функціи

$$f(x) = a + a_1 x + \ldots + a_n x^n$$

дѣлятся на p, въ такомъ случаѣ говорятъ, что функція $f(x)$ сравнима съ нулемъ по модулю p, и выражаютъ это тожественнымъ сравненіемъ

$$f(x) \equiv 0 \pmod{p}.$$

Очевидно, что тожественному сравненію удовлетворяетъ всякое число x; но нельзя утверждать обратное; такъ, сравненіе

$$x^p - x \equiv 0 \pmod{p}$$

удовлетворяется всякимъ числомъ, а между тѣмъ оно не тожество.

Двѣ функціи, сравнимыя порознь съ третьею, очевидно сравнимы между собою. Поэтому всѣ функціи сравнимыя съ одной какой нибудь функціею $f(x)$, составляютъ особый классъ функцій сравнимыхъ между собой, каждая съ каждой. Такія функціи мы согласимся не считать за различныя.

Въ выраженіи функціи, разсматриваемой по модулю p, коэффиціенты могутъ быть соотвѣтственно замѣняемы какими угодно ихъ вычетами; вслѣдствіе этого всякую функцію можно привести къ такому простѣйшему виду, гдѣ числовая величина каждаго коэффиціента будетъ $< p$ или даже $< \frac{p}{2}$, если только $p > 2$.

Наибольшая степень перемѣннаго x въ выраженіи $f(x)$, у

которой коэффиціентъ не дѣлится на p, называется степенью функціи $f(x)$ по модулю p. Такъ, напримѣръ, степень функціи

$$10x^3 - 2x^2 + 7x - 4$$

по модулю 2 есть 1; по модулю 5 есть 2; по модулю 7 есть 3.

Степень функціи по модулю p очевидно равна абсолютной степени функціи въ ея простѣйшемъ видѣ. Для предыдущей функціи имѣемъ такія тожества:

$$10x^3 - 2x^2 + 7x - 4 \equiv x \pmod{2},$$
$$10x^3 - 2x^2 + 7x - 4 \equiv 3x^2 - 2x + 1 \pmod{5},$$
$$10x^3 - 2x^2 + 7x - 4 \equiv 3x^3 - 2x^2 + 3 \pmod{7}.$$

Функція нулевой степени въ простѣйшемъ своемъ выраженіи приводится къ одному изъ чиселъ $0, 1, 2, \ldots p-1$, если p означаетъ модуль. Всякая функція первой степени по модулю p приводится къ виду

$$ax + b,$$

причемъ a и b могутъ имѣть слѣдующія значенія:

$$a = 1, 2, 3, \ldots p-1,$$
$$b = 0, 1, 2, \ldots p-1.$$

Слѣдовательно число различныхъ функцій первой степени по модулю p есть $p(p-1)$.

Всѣ представители функцій второй степени получаются изъ формулы

$$ax^2 + bx + c,$$

давая для a, b, c значенія

$$a = 1, 2, 3, \ldots p-1,$$
$$b = 0, 1, 2, \ldots p-1,$$
$$c = 0, 1, 2, \ldots p-1;$$

слѣдовательно число такихъ функцій равно $p^2(p-1)$.

Вообще, число различныхъ функцій n-ой степени по модулю p есть $p^n(p-1)$.

70. Изъ первыхъ четырехъ дѣйствій надъ функціями, по модулю p, особеннаго поясненія требуетъ только дѣленіе; имъ теперь мы займемся.

Дѣлить по модулю p функцію степени n,

$$f(x) = Ax^n + A_1x^{n-1} + \ldots + A_n,$$

на функцію степени $m \leqq n$,

$$F(x) = Bx^m + B_1x^{m-1} + \ldots + B_m,$$

значитъ искать такую третью функцію $\varphi(x)$, чтобъ разность между произведеніемъ $F(x)\varphi(x)$ и функціей $f(x)$ по модулю p была степени ниже m.

Функція $\varphi(x)$ называется частнымъ, а разность

$$f(x) - F(x)\,\varphi(x) = r(x)$$

остаткомъ отъ дѣленія по модулю p функціи $f(x)$ на $F(x)$.

Прежде всего слѣдуетъ здѣсь доказать, что не можетъ существовать двухъ рѣшеній. Но убѣдиться въ этомъ очень легко. Допустивъ, что существуетъ два частныхъ $\varphi(x)$ и $\varphi_1(x)$, различныхъ по модулю p, мы будемъ имѣть двѣ функціи

$$r(x) \equiv f(x) - F(x)\,\varphi(x) \pmod{p},$$

$$r_1(x) \equiv f(x) - F(x)\,\varphi_1(x) \pmod{p}$$

каждая степени ниже m по модулю p, разность которыхъ будетъ представлять функцію также степени ниже m по модулю p. Вычитая послѣднія два сравненія одно изъ другаго, получаемъ тожество

$$(1) \ldots \; r(x) - r_1(x) \equiv F(x)\,\big(\varphi_1(x) - \varphi(x)\big) \pmod{p},$$

вторая часть котораго представляетъ функцію степени не ниже m, ибо разность $\varphi_1(x) - \varphi(x)$, по предположенію, не сравнима съ

нулемъ; между тѣмъ первая часть есть функція степени ниже m. Поэтому сравненіе (1) не можетъ быть тожественнымъ, и предположеніе существованія двухъ различныхъ частныхъ невозможно.

Для опредѣленія частнаго и остатка слѣдуетъ поступать такъ:

Если коеффиціентъ B въ дѣлителѣ не равенъ 1, мы найдемъ число B', которое удовлетворяло бы сравненію

$$BB' \equiv 1 \pmod{p},$$

и положивъ

$$B'F(x) \equiv x^m + B'_1 x^{m-1} + \ldots + B'_m \pmod{p},$$

будемъ дѣлить функцію $f(x)$ на функцію

$$F_1(x) = x^m + B'_1 x^{m-1} + \ldots + B'_m$$

по обыкновенному алгебрическому правилу съ добавленіемъ однако, что въ получаемыхъ остаткахъ каждый коеффиціентъ дозволяется замѣнять какимъ угодно его вычетомъ по модулю p. Этимъ можно воспользоваться такъ, что числовыя величины коеффиціентовъ въ остаткахъ не превзойдутъ никогда p или даже $\frac{p}{2}$. Когда дойдемъ до остатка $r(x)$ степени ниже m, дѣйствіе будетъ окончено. Обозначивъ частное чрезъ $\varphi_1(x)$, мы замѣчаемъ, что коеффиціенты въ $\varphi_1(x)$ будутъ цѣлыми и при томъ будемъ имѣть равенство слѣдующаго вида:

$$f(x) = F_1(x)\,\varphi_1(x) + r(x) + p\psi(x).$$

Здѣсь $p\psi(x)$ изображаетъ цѣлую функцію съ коеффиціентами дѣлящимися на p; она произошла отъ дозволенной замѣны коеффиціентовъ въ остаткахъ ихъ вычетами по модулю p, и выраженіе ея, конечно, будетъ зависѣть отъ того, какъ мы воспользовались этимъ правомъ измѣненія значеній коеффиціентовъ. Но во всякомъ случаѣ послѣднее равенство можно написать въ видѣ такого тожественнаго сравненія

$$f(x) \equiv F_1(x)\,\varphi_1(x) + r(x) \pmod{p}.$$

Отсюда, замѣчая, что $1 \equiv BB'$ (mod. p), выводимъ

$$f(x) \equiv BF_1(x) \cdot B'\varphi_1(x) + r(x) \text{ (mod. } p).$$

Изъ тожественнаго сравненія

$$F_1(x) \equiv B'F(x) \text{ (mod. } p)$$

выводимъ

$$BF_1(x) \equiv F(x) \text{ (mod. } p);$$

слѣдовательно

$$f(x) \equiv F(x) \cdot B'\varphi_1(x) + r(x) \text{ (mod. } p).$$

Называя для сокращенія

$$\varphi(x) = B'\varphi_1(x),$$

получаемъ

(2). . . . . $f(x) \equiv F(x)\ \varphi(x) + r(x)$ (mod. p).

Результатъ этотъ показываетъ, что функціи $\varphi(x)$ и $r(x)$, полученныя вышеуказаннымъ способомъ суть искомыя, именно, первая составляетъ частное, вторая остатокъ отъ дѣленія по модулю p функціи $f(x)$ на $F(x)$.

Если случится, что всѣ коэффиціенты въ выраженіи остатка $r(x)$ дѣлятся на p, то сравненіе (2) приметъ видъ

(3). . . . . $f(x) \equiv F(x)\ \varphi(x)$ (mod. p).

Тогда говорятъ, что по модулю p функція $f(x)$ дѣлится безъ остатка на $F(x)$, или, что $F(x)$ есть дѣлителемъ функціи $f(x)$.

Примѣръ. Чтобы раздѣлить по модулю 17 функцію

$$f = 5x^4 - 7x^3 + 5x^2 - 6x + 3$$

на

$$F = 3x^2 + 7x - 1,$$

мы умножаемъ предварительно дѣлитель на 6; получаемъ

$$6F \equiv x^2 + 8x - 6 \text{ (mod. } 17).$$

Затѣмъ дѣлимъ f на функцію $x^2 + 8x - 6$

$$\begin{array}{rrrrr|l}
5x^4 - & 7x^3 + & 5x^2 - & 6x + & 3 & x^2 + 8x - 6 \\
-5x^4 - & 40x^3 + & 30x^2 & & & \overline{5x^2 + 4x + 3} \\
\hline
 & -47x^3 + & 35x^2 - & 6x + & 3 & \\
 & \equiv 4x^3 + & x^2 - & 6x + & 3 & \\
 & - 4x^3 - & 32x^2 + & 24x & & \\
\hline
 & & -31x^2 + & 18x + & 3 & \\
 & & \equiv 3x^2 + & x + & 3 & \\
 & & - 3x^2 - & 24x + & 18 & \\
\hline
 & & & -23x + & 21 & \\
 & & & \equiv 11x + & 4. &
\end{array}$$

Здѣсь каждый остатокъ выписанъ два раза: въ первоначальномъ его видѣ и затѣмъ въ простѣйшемъ видѣ. Результатъ дѣленія выражается тожественнымъ сравненіемъ

$$f \equiv 6F(5x^2 + 4x + 3) + 11x + 4 \pmod{17}$$

или, проще,

$$f \equiv F(13x^2 + 7x + 1) + 11x + 4 \pmod{17}.$$

Отсюда видно, что искомое частное есть

$$13x^2 + 7x + 1,$$

а остатокъ

$$11x + 4.$$

71. Обозначивъ чрезъ a какое угодно число не дѣлящееся на p, а чрезъ a' другое число, удовлетворяющее условію

$$aa' \equiv 1 \pmod{p},$$

мы замѣчаемъ, что, какова бы ни была функція $f(x)$, всегда имѣетъ мѣсто тожество

$$f(x) \equiv aa'f(x) \pmod{p}.$$

Это показываетъ, что a есть дѣлитель функціи $f(x)$ по модулю p. Слѣдовательно всякое цѣлое число, не дѣлящееся на модуль, дѣлитъ по этому модулю всякую функцію; такъ что, по отношенію дѣлимости функцій по модулю p, каждое изъ чиселъ $1, 2, \ldots p-1$ играетъ такую же роль, какъ единица.

Если функція $F(x)$ дѣлитъ $f(x)$, то, каково бы ни было число a, если только оно не дѣлится на p, произведеніе $aF(x)$ будетъ также дѣлить функцію $f(x)$. Слѣдовательно, когда рѣчь идетъ о дѣлимости одной функціи на другую, можно не обращать вниманія на числовые множители дѣлителей; ихъ можно вводить или откидывать, смотря по желанію, и всегда можно предположить, если это понадобится, что въ выраженіи дѣлителя n-ой степени коеффиціентъ у x^n равенъ 1.

Большаго вниманія заслуживаетъ слѣдующая теорема.

Теорема. *Если произведеніе $f(x)\,f_1(x)$ сравнимо съ нулемъ по модулю p, то по крайней мѣрѣ одна изъ функцій $f(x)$, $f_1(x)$ сравнима съ нулемъ по тому же модулю p.*

На самомъ дѣлѣ, допустимъ, что ни одна изъ функцій $f(x)$, $f_1(x)$ не сравнима съ нулемъ по модулю p; тогда, пренебрегая членами, коеффиціенты которыхъ дѣлятся на p, мы могли бы положить

$$f(x) = ax^n + \ldots,$$

$$f_1(x) = bx^m + \ldots,$$

гдѣ n и m изображаютъ степени $f(x)$ и $f_1(x)$, и поэтому $n \geqq 0$, $m \geqq 0$, при томъ ни a ни b не дѣлятся на p. Внося эти выраженія въ сравненіе $f(x)\,f(x_1) \equiv 0 \pmod{p}$, получаемъ

$$abx^{m+n} + \ldots \equiv 0 \pmod{p},$$

откуда заключаемъ

$$ab \equiv 0 \pmod{p}.$$

Но это невозможно, ибо ни a ни b не дѣлится на p; слѣдо-

вательно и то невозможно, чтобы ни одна изъ функцій $f(x)$, $f_1(x)$ не была сравнима съ нулемъ по модулю p.

72. Къ вопросу объ общихъ дѣлителяхъ по модулю p двухъ какихъ нибудь данныхъ функцій примѣняется непосредственно принципъ Эвклида; вслѣдствіе этого получается возможность составить основанія теоріи дѣлимости функцій по данному модулю.

Возьмемъ двѣ функціи $f(x)$ и $F(x)$, изъ коихъ вторая степени не выше первой, и раздѣливъ по модулю p функцію $f(x)$ на $F(x)$, обозначимъ частное чрезъ Q_1, а остатокъ чрезъ $c_1\, r_1(x)$, предполагая при этомъ, что коеффиціентъ у наивысшей степени x въ $r_1(x)$ равенъ 1, и что число c_1 не дѣлится на p. Затѣмъ раздѣлимъ по модулю p функцію $F(x)$ на $r_1(x)$; частное обозначимъ чрезъ Q_2, а остатокъ чрезъ $c_2\, r_2(x)$, при чемъ c_2 не дѣлится на p, а коеффиціентъ у наивысшей степени x въ $r_2(x)$ равенъ 1. Послѣ этого раздѣлимъ $r_1(x)$ на $r_2(x)$, и будемъ продолжать такимъ образомъ дѣйствовать до тѣхъ поръ, пока не дойдемъ до остатка тожественно сравнимаго съ нулемъ.

Пусть въ ряду полученныхъ остатковъ $c_n\, r_n(x)$ изображаетъ послѣдній; степень $r_n(x)$ можетъ равняться нулю, тогда $r_n(x) \equiv 1$; для отличія обозначимъ $r_n(x)$ буквою D, и напишемъ рядъ тожествъ

$$(1)\ldots\ldots\left\{\begin{array}{r} f(x) \equiv F(x)\, Q_1 + c_1\, r_1(x) \\ F(x) \equiv r_1(x)\, Q_2 + c_2\, r_2(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ r_{n-2}(x) \equiv r_{n-1}(x)\, Q_n + c_n D \\ r_{n-1}(x) \equiv D Q_{n+1} \end{array}\right\} \pmod{p}.$$

Умножая обѣ части каждаго изъ нихъ соотвѣтственно на числа $c'_1, c'_2, \ldots c'_n$, 1, удовлетворяющія условіямъ

$$c_1\, c'_1 \equiv c_2\, c'_2 \equiv \ldots \equiv c_n\, c'_n \equiv 1 \pmod{p},$$

получаемъ

$$(2) \ldots\ldots \left\{ \begin{array}{l} c'_1 f(x) \equiv c'_1 F(x)\, Q_1 + r_1(x) \\ c'_2 F(x) \equiv c'_2 r_1(x)\, Q_2 + r_2(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c'_n r_{n-2}(x) \equiv c'_n r_{n-1}(x)\, Q_n + D \\ r_{n-1}(x) \equiv D Q_{n+1} \end{array} \right\} (\mathrm{mod.}\ p).$$

Въ системѣ (1) съ помощью послѣдняго сравненія изъ предшествующихъ можно исключить $r_{n-1}(x)$. Послѣ этого предпослѣднее сравненіе дастъ возможность исключить изъ предшествующихъ сравненій функцію $r_{n-2}(x)$. Продолжая такимъ образомъ исключать послѣдовательно $r_{n-3}(x)$, $r_{n-4}(x)$, . . . , мы наконецъ дойдемъ до третьяго сравненія, которое дастъ возможность исключить изъ первыхъ двухъ остатокъ $r_1(x)$; тогда эти послѣднія сравненія представятся въ такомъ видѣ:

$$(3) \ldots\ldots\ldots\ldots \left\{ \begin{array}{l} f(x) \equiv UD \\ F(x) \equiv VD \end{array} \right\} (\mathrm{mod.}\ p),$$

гдѣ U и V изображаютъ цѣлыя функціи съ цѣлыми коеффиціентами.

Переходя теперь къ системѣ (2) мы замѣчаемъ, что первое сравненіе позволяетъ исключить изъ остальныхъ остатокъ $r_1(x)$. Послѣ этого второе сравненіе дастъ возможность исключить $r_2(x)$ изъ послѣдующихъ сравненій. Продолжая такимъ образомъ послѣдовательныя исключенія, дойдемъ наконецъ до $(n-1)$-го сравненія, которое дастъ возможность исключить изъ двухъ послѣднихъ сравненій остатокъ $r_{n-1}(x)$. Тогда предпослѣднее сравненіе приметъ очевидно такой видъ:

$$(4) \ldots\ldots\ldots\; X f(x) + Y F(x) \equiv D\ (\mathrm{mod.}\ p),$$

гдѣ X и Y изображаютъ цѣлыя функціи.

Изъ (4) слѣдуетъ прямо, что всякій общій дѣлитель по модулю p функцій $f(x)$ и $F(x)$ будетъ также дѣлителемъ D; изъ (3) вытекаетъ обратное предложеніе: всякій дѣлитель D есть общій дѣлитель функцій $f(x)$ и $F(x)$. Функція D называется поэтому общимъ наибольшимъ дѣлителемъ по модулю p функцій $f(x)$ и $F(x)$.

Если $D=1$, въ такомъ случаѣ функціи $f(x)$ и $F(x)$, кромѣ очевидныхъ общихъ дѣлителей $1, 2, 3, \ldots p-1$, другихъ не имѣютъ; тогда говорятъ, что онѣ взаимно простыя по модулю p.

Зная, какъ находить общій наибольшій дѣлитель двухъ функцій, мы тѣмъ самымъ знаемъ, какъ найти общій наибольшій дѣлитель какого угодно числа функцій по данному модулю.

Изъ всѣхъ функцій, дѣлящихся по модулю p на обѣ функціи $f(x)$ и $F(x)$, та, степень которой самая низкая, называется наименьшимъ кратнымъ $f(x)$ и $F(x)$ по модулю p. Она опредѣляется по формулѣ

$$M \equiv \frac{f(x)\,F(x)}{D} \pmod{p}.$$

Относительно функцій взаимно простыхъ по модулю p сохраняютъ справедливость всѣ основныя теоремы, относящіяся къ взаимно простымъ числамъ, именно:

1°. *Если $f(x)$ и $F(x)$ суть взаимно простыя по модулю p, то существуютъ двѣ цѣлыя функціи X и Y, удовлетворяющія сравненію*

$$Xf(x) + YF(x) \equiv 1 \pmod{p}.$$

2°. *Если каждая изъ функцій $f_1(x), f_2(x), \ldots f_m(x)$ есть простая съ $F(x)$ по модулю p, то произведеніе $f_1(x)\,f_2(x) \ldots f_m(x)$ представляетъ функцію простую съ $F(x)$ по модулю p.*

3°. *Если функція $f(x)$ дѣлится по модулю p на каждую изъ функцій $F_1(x), F_2(x), \ldots F_m(x)$, а эти послѣднія суть простыя, каждая относительно каждой, то $f(x)$ дѣлится по модулю p на произведеніе $F_1(x)\,F_2(x) \ldots F_m(x)$.*

73. Если функція не имѣетъ по модулю p другихъ дѣлителей кромѣ самой себя и 1, 2, 3, . . . $p-1$, то ее называютъ *неприводимой по модулю p*.

Если функція $f(x)$ неприводима, то при всякомъ числѣ a, не дѣлящемся на p, произведеніе $af(x)$ представитъ функцію также неприводимую по модулю p. По отношенію къ неприводимости, какъ характеристической чертѣ, мы согласимся не считать за различныя такія функціи, которыя отличаются между собою только постоянными множителями.

Простѣйшія неприводимыя функціи суть первой степени, именно:

$$x,\ x\pm1,\ x\pm2, \ldots x\pm\frac{p-1}{2},$$

а въ случаѣ $p=2$:

$$x,\ x-1.$$

Неприводимыя функціи, по отношенію къ другимъ функціямъ, разсматриваемымъ по модулю p, играютъ такую же роль, какъ въ ариѳметикѣ простыя числа. Мы не станемъ повторять здѣсь извѣстныхъ доказательствъ; ограничимся только перечисленіемъ основныхъ предложеній.

1°. *Если произведеніе $f_1(x)\, f_2(x) \ldots f_m(x)$ дѣлится по модулю p на неприводимую функцію $f(x)$, то по крайней мѣрѣ одинъ изъ множителей $f(x)$, $f_1(x), \ldots f_m(x)$ дѣлится по модулю p на $f(x)$.*

2°. *Всякая функція разлагается по модулю p на произведеніе неприводимыхъ множителей однимъ только образомъ.*

3°. *Для того чтобы функція $f(x)$ дѣлилась по модулю p на $F(x)$ необходимо и достаточно условіе, чтобы каждый изъ неприводимыхъ множителей, входящихъ въ составъ $F(x)$, входилъ въ составъ $f(x)$ съ показателемъ не ниже чѣмъ въ $F(x)$.*

Нахожденіе общаго наибольшаго дѣлителя равно какъ и наименьшаго кратнаго нѣсколькихъ функцій, по модулю p, съ помощью разложенія этихъ функцій на неприводимые множи-

тели, совершается такимъ же образомъ, какъ для цѣлыхъ чиселъ, которыхъ составъ извѣстенъ.

74. Разложеніе какой либо функціи на неприводимые множители

$$f(x) \equiv P_1^{m_1} P_2^{m_2} \ldots P_r^{m_r} \pmod{p}$$

можетъ быть всегда выполнено посредствомъ конечнаго числа дѣйствій. Это очевидно, ибо число различныхъ функцій по модулю p, степень которыхъ ниже n, конечно. Обозначая соотвѣтственно чрезъ $n, n_1, n_2, \ldots$ степени функцій $f(x)$, P_1, $P_2, \ldots$, имѣемъ

$$n = m_1 n_1 + m_2 n_2 + \ldots + m_r n_r.$$

Для опредѣленія P_1, $P_2, \ldots$, въ случаѣ если одно изъ чиселъ p или n довольно значительно, приходится испытывать огромное число функцій. Были дѣланы попытки для устраненія, хотя бы отчасти, этого неудобства, но мы не станемъ вдаваться здѣсь въ изысканія этого рода.

Неприводимые множители P_1, $P_2, \ldots$, входящіе въ составъ функціи $f(x)$, слѣдуетъ различать на простые и кратные, смотря по показателямъ m_1, $m_2, \ldots$ Сообразно этому и вопросъ о разложеніи функціи на неприводимые множители можно раздѣлить на два: объ отыскиваніи кратныхъ неприводимыхъ множителей и, второй, объ отыскиваніи простыхъ неприводимыхъ множителей. Первый изъ нихъ приводится ко второму, такъ что разложеніе данной функціи на неприводимые множители окончательно всегда приводится къ разложенію одной или нѣсколькихъ функцій, не имѣющихъ вовсе кратныхъ неприводимыхъ множителей.

Но прежде, чѣмъ это доказать, провѣримъ справедливость слѣдующей леммы.

Лемма. *Какова бы ни была функція $f(x)$, всегда имѣетъ мѣсто тожество*

$$f(x)^{p^n} \equiv f(x^{p^n}) \pmod{p}.$$

Дѣйствительно, допустимъ сначала, что функція $f(x)$ есть первой степени

$$f(x) = a_0 + a_1 x;$$

въ такомъ случаѣ находимъ

$$f(x)^p = a_0^p + \frac{p}{1} a_0^{p-1} a_1 x + \frac{p(p-1)}{1.2} a_0^{p-2} a_1^2 x^2 + \ldots + a_1^p x^p.$$

Замѣчая, что всѣ коеффиціенты во второй части, за исключеніемъ двухъ крайнихъ, дѣлятся на p, мы можемъ послѣднее равенство написать въ видѣ сравненія такъ:

$$f(x)^p \equiv a_0^p + a_1^p x^p \ (\text{mod.}\ p).$$

Но по теоремѣ Фермата имѣемъ

$$a_0^p \equiv a_0; \ a_1^p \equiv a_1 \ (\text{mod.}\ p);$$

слѣдовательно

$$f(x)^p \equiv a_0 + a_1 x^p \ (\text{mod.}\ p),$$

или

$$(1) \ldots \ldots \ldots \ldots f(x)^p \equiv f(x^p) \ (\text{mod.}\ p).$$

Допустимъ теперь, что сравненіе (1) доказано для всякой функціи $f(x)$ n-ой степени, и примемъ во вниманіе какую угодно функцію $(n+1)$-ой степени

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n + a_{n+1} x^{n+1}.$$

Обозначивъ чрезъ $\varphi(x)$ функцію

$$\varphi(x) = a_0 + a_1 x + \ldots + a_n x^n,$$

имѣемъ

$$f(x) = \varphi(x) + a_{n+1} x^{n+1},$$

откуда выводимъ

$$f(x)^p = \varphi(x)^p + \frac{p}{1} \varphi(x)^{p-1} a_{n+1} x^{n+1} + \ldots + a^p_{n+1} x^{p(n+1)}.$$

Равенство это можно написать въ видѣ сравненія

$$f(x)^p \equiv \varphi(x)^p + a^p_{n+1} x^{p(n+1)} \pmod{p}.$$

Но по предположенію имѣемъ

$$\varphi(x)^p \equiv \varphi(x^p) \pmod{p},$$

а по теоремѣ Фермата

$$a^p_{n+1} \equiv a_{n+1} \pmod{p};$$

слѣдовательно

$$f(x)^p \equiv \varphi(x^p) + a_{n+1} x^{p(n+1)} \pmod{p},$$

или, одно и то же,

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

Итакъ, сравненіе (1), будучи справедливымъ для функцій n-ой степени, оказывается справедливымъ и для функцій $(n+1)$-ой степени. А такъ какъ оно уже доказано нами для $n = 1$, то слѣдовательно оно имѣетъ мѣсто при всякомъ n.

Возвышая теперь обѣ части (1) въ степень p, получаемъ

$$f(x)^{p^2} \equiv f(x^p)^p \pmod{p};$$

внося въ обѣ части того же сравненія (1) x^p на мѣсто x, получаемъ

$$f(x^p)^p \equiv f(x^{p^2}) \pmod{p}.$$

Сличая послѣднее сравненіе съ предыдущимъ, заключаемъ

(2). . . . . $f(x)^{p^2} \equiv f(x^{p^2}) \pmod{p}$.

Возвышая обѣ части (2) въ степень p, получаемъ

$$f(x)^{p^3} \equiv f(x^{p^2})^p \pmod{p};$$

но изъ (1) выводимъ

$$f(x^{p^3})^p \equiv f(x^{p^3}) \pmod{p},$$

слѣдовательно

$$(3) \ldots\ldots\ldots\ldots \quad f(x)^{p^3} \equiv f(x^{p^3}) \pmod{p}.$$

Продолжая дѣйствовать подобнымъ образомъ далѣе, мы приходимъ къ общей формулѣ

$$f(x)^{p^n} \equiv f(x^{p^n}) \pmod{p}.$$

Что и слѣдовало доказать.

75. Возвращаясь къ разложенію функціи на неприводимые множители, мы обратимъ вниманіе на составъ общаго наибольшаго дѣлителя D функціи

$$(1) \ldots\ldots\ldots \quad f(x) \equiv P_1^{m_1} P_2^{m_2} \ldots P_r^{m_r} \pmod{p}$$

и ея производной

$$f'(x) \equiv P_1^{m_1-1} P_2^{m_2-1} \ldots P_r^{m_r-1} \Big[m_1 P_1' P_2 \ldots P_r + m_2 P_1 P_2' \ldots P_r + \ldots$$
$$+ m_r P_1 P_2 \ldots P_r' \Big] \pmod{p}.$$

Если m_1 не дѣлится на p, то P_1 войдетъ въ составъ D съ показателемъ $m_1 - 1$, ибо тогда функція въ скобкахъ во второй части не дѣлится на P_1; напротивъ, если m_1 дѣлится на p, то P_1 войдетъ въ составъ D съ показателемъ m_1. Сказанное примѣняется ко всѣмъ прочимъ множителямъ P_2, $P_3, \ldots$

Если $m_1 = m_2 = \ldots = m_r = 1$, то функціи $f(x)$ и $f'(x)$ относительно простыя; тогда $D = 1$.

Положимъ, вообще, что въ ряду показателей $m_1, m_2, \ldots m_r$ число такихъ, которые дѣлятся на p, равно i. Обозначивъ ихъ чрезъ $m_1, m_2, \ldots m_i$, имѣемъ

$$m_1 = n_1 p, \; m_2 = n_2 p, \ldots m_i = n_i p,$$

$$(2) \ldots \quad D \equiv U^p P_{i+1}^{m_{i+1}-1} P_{i+2}^{m_{i+2}-1} \ldots P_r^{m_r} \pmod{p},$$

при чемъ

$$U \equiv P_1^{n_1} P_2^{n_2} \ldots P_i^{n_i} \pmod{p}.$$

Если согласимся обозначать соотвѣтственно чрезъ X_1, $X_2, \ldots X_k$ произведеніе тѣхъ функцій въ ряду

$$P_{i+1},\ P_{i+2}, \ldots P_r,$$

которыя въ составъ $f(x)$ входятъ съ показателемъ $1, 2, \ldots k$, то сравненія (1) и (2) можно написать такъ:

(3). . . . . . $f(x) \equiv U^p X_1 X_2^2 X_3^3 \ldots X_k^k \pmod{p}$,

(4). . . . . . . $D \equiv U^p X_2 X_3^2 \ldots X_k^{k-1} \pmod{p}$.

Въ случаѣ, еслибы ни одинъ изъ показателей $m_1, m_2, \ldots m_r$ не дѣлился на p, слѣдовало бы положить $U = 1$; въ случаѣ отсутствія простыхъ неприводимыхъ множителей мы имѣли бы $X_1 = 1$ и т. д. X_p, $X_{2p}, \ldots$ всегда изображаютъ 1.

Называя чрезъ D_1 общій наибольшій дѣлитель по модулю p, составленный для функціи D и ея производной D', имѣемъ по формулѣ (4)

(5). . . . . . . $D_1 \equiv U^p X_3 X_4^2 \ldots X_k^{k-2} \pmod{p}$.

По той же формулѣ общій наибольшій дѣлитель функцій D_1 и D_1' выражается такъ:

(6). . . . . $D_2 \equiv U^p X_4 \ldots X_k^{k-3} \pmod{p}$.

Такъ поступая далѣе, дойдемъ наконецъ до функціи

(7) . . . . $D_{k-1} \equiv U^p \pmod{p}$,

производная которой по модулю p сравнима съ нулемъ.

Опредѣливъ функціи $D, D_1, \ldots D_{k-1}$ по способу Эвклида, мы имѣемъ $k+1$ сравненій (3), (4), . . . (7), содержащихъ $k+1$ неизвѣстныхъ U, X_1, $X_2, \ldots X_k$.

На основаніи вышедоказанной леммы, изъ (7) заключаемъ, что въ выраженіи функціи D_{k-1} показатели у различныхъ степеней x дѣлятся на p. Полагая слѣдовательно

$$D_{k-1} = a_0 + a_1 x^p + a_2 x^{2p} + \ldots,$$

изъ (7) выводимъ

$$U \equiv a_0 + a_1 x + a_2 x^2 + \ldots \pmod{p}.$$

Найдя такимъ образомъ U, мы раздѣляемъ каждую изъ функцій $f(x)$, D, $D_1, \ldots D_{k-2}$ на U^p, или, одно и то же, на функцію

$$a_0 + a_1 x^p + a_2 x^{2p} + \ldots$$

Обозначая частныя, получаемыя при этомъ, чрезъ $E, E_1, \ldots E_{k-1}$, имѣемъ

$$\left.\begin{array}{l} E \equiv X_1 X_2^2 \ldots X_k^k \\ E_1 \equiv X_2 X_3^2 \ldots X_k^{k-1} \\ E_2 \equiv X_3 \ldots X_k^{k-2} \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ E_{k-1} \equiv X_k \end{array}\right\} \pmod{p}.$$

Раздѣляя, по модулю p, функцію E на E_1, затѣмъ E_1 на E_2, послѣ этого E_2 на E_3 и т. д., и называя получаемыя при этомъ частныя чрезъ $G_1, G_2, \ldots G_k$, имѣемъ

$$\left.\begin{array}{l} G \equiv X_1 X_2 \ldots X_k \\ G_1 \equiv X_2 \ldots X_k \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ G_{k-2} \equiv X_{k-1} X_k \\ G_{k-1} \equiv X_k \end{array}\right\} \pmod{p}.$$

Наконецъ, раздѣлимъ функцію G на G_1, затѣмъ G_1 на G_2, G_2 на G_3 и т. д.; получимъ рядъ частныхъ $H, H_1, \ldots H_{k-1}$, которыя будутъ равняться искомымъ функціямъ $X_1, X_2, \ldots X_k$.

$$\left.\begin{aligned} H &\equiv X_1 \\ H_1 &\equiv X_2 \\ &\cdots\cdots \\ &\cdots\cdots \\ H_{k-2} &\equiv X_{k-1} \\ H_{k-1} &\equiv X_k \end{aligned}\right\} (\mathrm{mod.}\ p).$$

Разложеніе функціи $f(x)$ на неприводимые множители сведено такимъ образомъ на разложеніе функцій $X_1, X_2, \ldots X_k, U$, изъ коихъ только послѣдняя можетъ содержать въ своемъ составѣ равные неприводимые множители. Относительно этой функціи мы можемъ поступать точно также, какъ поступали съ функціей $f(x)$, и очевидно, что окончательно вопросъ приведется къ разложенію такихъ только функцій, которыя не допускаютъ кратныхъ множителей.

Примѣръ 1. Полагая $p=5$, возьмемъ во вниманіе функцію

$$f \equiv x^{10} + x^9 - x^8 - x^6 - x^5 - 2x^4 + 2x^3 + 2x - 2 \ (\mathrm{mod.}\ 5).$$

Производная ея выражается по формулѣ

$$f' \equiv -x^8 + 2x^7 - x^5 + 2x^3 + x^2 + 2 \ (\mathrm{mod.}\ 5).$$

Общій наибольшій дѣлитель f и f' равенъ

$$D \equiv x^7 - x^6 - x^5 - 2x^2 + 2x + 2 \ (\mathrm{mod.}\ 5).$$

Производная функціи D опредѣляется формулой

$$3D' \equiv x^6 + 2x^5 + 3x + 1 \ (\mathrm{mod.}\ 5).$$

Общій наибольшій дѣлитель D и D' равенъ

$$D_1 \equiv 3D' \equiv x^6 + 2x^5 + 3x + 1 \ (\mathrm{mod.}\ 5).$$

Далѣе получаемъ

$$D_1' \equiv x^5 - 2 \pmod{5},$$

$$D_2 \equiv D_1' \equiv x^5 - 2 \pmod{5},$$

$$D_2' \equiv 0 \pmod{5}.$$

Отсюда заключаемъ, что разложеніе функціи f на неприводимые множители по модулю 5 можно представить такъ:

$$f \equiv U^5 X_1 X_2^2 X_3^3 \pmod{5},$$

при чемъ имѣемъ

$$U \equiv x - 2 \pmod{5}.$$

Для полученія другихъ множителей имѣемъ сравненія

$$D \equiv U^5 X_2 X_3^2 \pmod{5},$$

$$D_1 \equiv U^5 X_3 \pmod{5}.$$

Изъ нихъ дѣленіемъ выводимъ

$$X_1 X_2 X_3 \equiv \frac{f}{D} \equiv x^3 + 2x^2 + 2x - 1 \pmod{5},$$

$$X_2 X_3 \equiv \frac{D}{D_1} \equiv x + 2 \pmod{5},$$

$$X_3 \equiv \frac{D_1}{U^5} \equiv x + 2 \pmod{5}.$$

Отсюда, опять дѣленіемъ, выводимъ

$$\left.\begin{array}{l} X_1 \equiv x^2 + 2 \\ X_2 \equiv 1 \\ X_3 \equiv x + 2 \end{array}\right\} \pmod{5}.$$

Слѣдовательно имѣемъ

$$f \equiv (x - 2)^5 (x^2 + 2)(x + 2)^3 \pmod{5}.$$

Примѣръ 2. Полагая

$$f \equiv x^9 + 4x^8 + 6x^7 - x^6 + 2x^5 - 6x^4 - 2x^3 - 6x^2 + x - 5 \pmod{11},$$

находимъ

$$\left.\begin{aligned} D &\equiv x^4 + 5x^3 - 2x^2 - 4x + 2 \\ D_1 &\equiv x^2 + 2x + 1 \\ D_2 &\equiv x + 1 \\ D_3 &\equiv 1 \end{aligned}\right\} \pmod{11}.$$

Разложеніе функціи f по модулю 11 представляется такъ:

$$f \equiv X_1\, X_2^2\, X_3^3\, X_4^4.$$

Послѣдовательнымъ дѣленіемъ находимъ

$$X_1\, X_2\, X_3\, X_4 \equiv \frac{f}{D} \equiv x^5 - x^4 + 2x^3 + 2x^2 + x + 3 \pmod{11},$$

$$X_2\, X_3\, X_4 \equiv \frac{D}{D_1} \equiv x^2 + 3x + 2 \pmod{11},$$

$$X_3\, X_4 \equiv \frac{D_1}{D_2} \equiv x + 1 \pmod{11},$$

$$X_4 \equiv D_2 \equiv x + 1 \pmod{11}.$$

Отсюда получаемъ

$$\left.\begin{aligned} X_1 &\equiv x^3 - 4x^2 + x - 4 \\ X_2 &\equiv x + 2 \\ X_3 &\equiv 1 \\ X_4 &\equiv x + 1 \end{aligned}\right\} \pmod{11};$$

слѣдовательно

$$f \equiv (x^3 - 4x^2 + x - 4)\,(x + 2)^2\,(x + 1)^4 \pmod{11}.$$

§ III. Новое доказательство теоремы Лагранжа. Пониженіе степени сравненія.

76. Если функція $f(x)$ неприводима по модулю p и степень ея выше единицы, то сравненіе

$$(1) \quad \ldots\ldots\ldots\ldots \quad f(x) \equiv 0 \ (\mathrm{mod.}\, p)$$

невозможно. Ибо допустивъ, что какое нибудь число a удовлетворяетъ ему, мы будемъ имѣть равенство

$$f(x) = (x - a)\,\varphi(x) + f(a),$$

которое, на основаніи того, что $f(a) \equiv 0 \ (\mathrm{mod.}\, p)$, приводитъ къ тожественному сравненію

$$f(x) \equiv (x - a)\,\varphi(x) \ (\mathrm{mod.}\, p),$$

показывающему, что, по модулю p, функція $f(x)$ дѣлится на $x - a$. Но это невозможно по предположенію.

Полагая, напротивъ,

$$f(x) \equiv P_1^{m_1} P_2^{m_2} \ldots P_r^{m_r} \ (\mathrm{mod.}\, p),$$

гдѣ $P_1, P_2, \ldots$ изображаютъ различные неприводимые дѣлители функціи $f(x)$, мы замѣчаемъ, что рѣшеніе сравненія (1) приводится къ рѣшенію отдѣльно каждаго изъ слѣдующихъ сравненій:

$$P_1 \equiv 0 \ (\mathrm{mod.}\, p),$$

$$P_2 \equiv 0 \ (\mathrm{mod.}\, p),$$

$$\ldots\ldots\ldots\ldots$$

$$P_r \equiv 0 \ (\mathrm{mod.}\, p).$$

Изъ нихъ только тѣ будутъ возможными, степень которыхъ равна 1; слѣдовательно число корней сравненія (1) равно числу различныхъ *линейныхъ* дѣлителей функціи $f(x)$ по модулю p.

Если $f(x)$ не дѣлится по модулю p ни на одну изъ функцій $x, x-1, x-2, \ldots x-p+1$, то сравненіе (1) невозможно.

77. **Теорема.** *Число рѣшеній сравненія*

$$f(x) \equiv 0 \pmod{p}$$

равно числу единицъ, заключающихся въ степени общаго наибольшаго дѣлителя D функцій $f(x)$ и $x^p - x$, составленнаго по модулю p. Всѣ эти рѣшенія найдутся изъ сравненія

$$D \equiv 0 \pmod{p}.$$

На самомъ дѣлѣ, по теоремѣ Фермата извѣстно, что сравненію

$$x^p - x \equiv 0 \pmod{p}$$

удовлетворяютъ числа

$$x = 0, 1, 2, \ldots p-1;$$

поэтому функція $x^p - x$ дѣлится по модулю p на каждую изъ функцій

$$x, x-1, x-2, \ldots x-p+1,$$

которыя просты между собою. Отсюда слѣдуетъ, что $x^p - x$ дѣлится на произведеніе $x(x-1)\ldots(x-p+1)$, то есть, имѣемъ такое сравненіе:

$$(1) \quad x^p - x \equiv x(x-1)(x-2)\ldots(x-p+1) \pmod{p}.$$

Оно было выведено нами раньше (n^0 68) съ помощью другихъ соображеній; теперь оно послужитъ для доказательства занимающей насъ теоремы. Положивъ, что въ составъ функціи

$$(2) \ldots\ldots\ldots f(x) \equiv P_1^{m_1} P_2^{m_2} \ldots P_r^{m_r} \pmod{p}$$

входитъ i неприводимыхъ дѣлителей первой степени, различныхъ между собой, мы обозначимъ ихъ чрезъ $P_1, P_2, \ldots P_i$; тогда изъ (1) и (2) выводимъ

$$D \equiv P_1 P_2 \ldots P_i \pmod{p},$$

и очевидно, что сравненіе

$$D \equiv 0 \pmod{p}$$

имѣетъ ровно i рѣшеній, то есть столько, сколько единицъ заключается въ его степени. Всѣ эти рѣшенія удовлетворяютъ сравненію

$$f(x) \equiv 0 \pmod{p},$$

которое не имѣетъ другихъ рѣшеній, кромѣ этихъ.

Такимъ образомъ наша теорема доказана.

Слѣдствіе 1. *Число рѣшеній сравненія не превышаетъ его степени.*

Ибо степень функціи D, какъ дѣлителя $f(x)$, не можетъ превышать степени $f(x)$.

Такъ мы получили вновь теорему Лагранжа.

Слѣдствіе 2. *Сравненіе* $f(x) \equiv 0 \pmod{p}$ *только тогда не имѣетъ рѣшенія, когда функціи* $f(x)$ *и* $x^p - x$ *суть относительно простыя по модулю* p.

Слѣдствіе 3. *Если степень* $f(x)$ *равна или больше* p, *то сравненіе* $f(x) \equiv 0 \pmod{p}$ *можетъ быть замѣнено сравненіемъ*

$$\varphi(x) \equiv 0 \pmod{p},$$

гдѣ $\varphi(x)$ *есть остатокъ отъ дѣленія, по модулю* p, *функціи* $f(x)$ *на* $x^p - x$.

Ибо тожественное сравненіе

$$f(x) \equiv (x^p - x) F(x) + \varphi(x) \pmod{p}$$

показываетъ прямо, что, по модулю p, общій наибольшій дѣлитель функцій $f(x)$ и $x^p - x$ есть тотъ же самый что и общій наибольшій дѣлитель функцій $\varphi(x)$ и $x^p - x$, другими словами, сравненія

$$f(x) \equiv 0 \pmod{p} \quad \text{и} \quad \varphi(x) \equiv 0 \pmod{p}$$

имѣютъ одинакія рѣшенія.

Слѣдствіе 4. *Число рѣшеній сравненія* $f(x) \equiv 0$ (mod. p) *тогда только равно его степени, когда функція* $x^p - x$, *по модулю* p, *дѣлится безъ остатка на* $f(x)$.

Ибо тогда только степень общаго наибольшаго дѣлителя функцій $x^p - x$ и $f(x)$ равна степени $f(x)$.

Примѣръ. Возьмемъ сравненіе

$$x^{17} - 7x - 1 \equiv 0 \text{ (mod. } 13).$$

Остатокъ отъ дѣленія первой его части на $x^{13} - x$ есть $x^5 - 7x - 1$. Слѣдовательно оно можетъ быть замѣнено такимъ:

$$x^5 - 7x - 1 \equiv 0 \text{ (mod. } 13).$$

Общій наибольшій дѣлитель функціи $x^5 - 7x - 1$ и $x^{13} - x$ есть $x^2 + 3x - 5$; поэтому окончательно наше сравненіе приводится къ такому:

$$x^2 + 3x - 5 \equiv 0 \text{ (mod. } 13).$$

Оно должно имѣть два рѣшенія, и на самомъ дѣлѣ находимъ, что числа $x = 3$ и $x = 7$ удовлетворяютъ ему; они удовлетворяютъ также и начальному сравненію.

§ IV. О двучленныхъ сравненіяхъ.

78. Разсматривая двучленное сравненіе

$$x^n - q \equiv 0 \text{ (mod. } p),$$

мы будемъ предполагать, что q не дѣлится на p. Въ противномъ случаѣ сравненіе имѣемъ одно только очевидное рѣшеніе $x = 0$, и не представляетъ тогда никакого интереса.

Принимая это къ свѣдѣнію, мы докажемъ слѣдующую теорему.

Теорема. *Чтобы сравненіе*

$$x^n \equiv q \pmod{p}$$

имѣло рѣшеніе, для этого необходимо и достаточно условіе

$$q^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

гдѣ d есть общій наибольшій дѣлитель чиселъ n и $p-1$.

Если оно удовлетворено, то сравненіе имѣетъ ровно d рѣшеній, и можетъ быть замѣнено сравненіемъ

$$x^d \equiv q^u \pmod{p},$$

гдѣ u изображаетъ число, удовлетворяющее условію

$$\frac{n}{d} u \equiv 1 \left(\bmod. \frac{p-1}{d}\right).$$

Доказательство этой теоремы состоитъ въ простомъ примѣненіи того, что было изложено въ предыдущемъ параграфѣ.

Прежде всего мы замѣчаемъ, что общій наибольшій дѣлитель D функцій $x^n - q$ и $x^p - x$ очевидно тотъ же самый что и функцій $x^n - q$ и $x^{p-1} - 1$. Но, обозначая чрезъ d общій наибольшій дѣлитель чиселъ n и $p-1$, мы можемъ написать

$$x^{n\frac{p-1}{d}} - q^{\frac{p-1}{d}} = (x^n - q) f_1(x),$$

$$x^{(p-1)\frac{n}{d}} - 1 = (x^{p-1} - 1) f_2(x),$$

гдѣ $f_1(x)$ и $f_2(x)$ суть цѣлыя функціи съ цѣлыми коеффиціентами. Отсюда, вычитая одно равенство изъ другаго, получаемъ

$$(x^n - q) f_1(x) - (x^{p-1} - 1) f_2(x) = 1 - q^{\frac{p-1}{d}}.$$

Результатъ этотъ показываетъ, что если условіе

(1). . . . . $q^{\frac{p-1}{d}} \equiv 1 \pmod{p}$

не будетъ удовлетворено, то $D = 1$.

Остается разсмотрѣть случай, когда условіе (1) удовлетворено. Тогда, опредѣливъ два положительныхъ числа u и v, удовлетворяющихъ условію

$$(2) \ldots\ldots\ldots\ldots nu-(p-1)v=d,$$

мы примемъ во вниманіе равенство

$$x^{nu}-q^u=(x^n-q)\,\varphi_1(x),$$

гдѣ $\varphi_1(x)$ есть цѣлая функція съ цѣлыми коеффиціентами. Оно, на основаніи (2), можетъ быть написано такъ:

$$x^d x^{(p-1)v}-q^u=(x^n-q)\,\varphi_1(x),$$

или такъ еще:

$$(3) \ldots\ldots x^d-q^u=(x^n-q)\,\varphi_1(x)-x^d(x^{(p-1)v}-1).$$

Обозначая частное отъ дѣленія функціи $x^d(x^{(p-1)v}-1)$ на $x^{p-1}-1$ чрезъ $\varphi_2(x)$, имѣемъ

$$x^d(x^{(p-1)v}-1)=(x^{p-1}-1)\,\varphi_2(x).$$

Внося это выраженіе во вторую часть (3), получаемъ

$$(4) \ldots\ldots x^d-q^u=(x^n-q)\,\varphi_1(x)-(x^{p-1}-1)\,\varphi_2(x).$$

Отсюда заключаемъ, что D есть дѣлитель x^d-q^u. Но не трудно убѣдиться, что $D=x^d-q^u$. Для этого стоитъ только показать, что функція x^d-q^u, по модулю p, дѣлитъ каждую изъ функцій x^n-q и $x^{p-1}-1$.

Дѣйствительно, изъ (1) и (2) вытекаетъ

$$\left.\begin{aligned} q &\equiv q^{\frac{un}{d}} \\ 1 &\equiv q^{\frac{u(p-1)}{d}} \end{aligned}\right\}(\mathrm{mod.}\,p),$$

на основаніи чего мы заключаемъ о справедливости двухъ тожественныхъ сравненій:

$$\left.\begin{aligned} x^n - q &\equiv (x^d)^{\frac{n}{d}} - (q^u)^{\frac{n}{d}} \\ x^{p-1} - 1 &\equiv (x^d)^{\frac{p-1}{d}} - (q^u)^{\frac{p-1}{d}} \end{aligned}\right\} (\mathrm{mod.}\, p).$$

Отсюда же видно ясно, что каждая изъ функцій

$$x^n - q \quad \text{и} \quad x^{p-1} - 1$$

дѣлится по модулю p на $x^d - q^u$.

Итакъ, смотря по тому будетъ ли условіе (1) удовлетворено или нѣтъ, мы будемъ имѣть $D = x^d - q^u$ или $D = 1$. Этотъ результатъ доказываетъ справедливость предложенной нами теоремы.

Смотря по тому возможно ли сравненіе $x^n \equiv q$ (mod. p), или невозможно, число q получаетъ названіе вычета или невычета n-ой степени.

Слѣдствіе 1. *Число вычетовъ n-ой степени по модулю p равно $\frac{p-1}{d}$; они суть корни сравненія*

$$x^{\frac{p-1}{d}} \equiv 1 \ (\mathrm{mod.}\ p).$$

Слѣдствіе 2. Если n число простое съ $p-1$, то сравненіе $x^n \equiv q$ (mod. p) имѣетъ одно только рѣшеніе, именно, $x \equiv q^u$ (mod. p).

Слѣдствіе 3. Если n дѣлитъ $p-1$, то сравненіе $x^n \equiv q$ (mod. p) имѣетъ n рѣшеній или ни одного, смотря по тому будетъ ли удовлетворено условіе $q^{\frac{p-1}{n}} \equiv 1$ (mod. p), или нѣтъ.

Слѣдствіе 4. Сравненіе $x^n \equiv 1$ (mod. p) имѣетъ всегда ровно d рѣшеній.

Слѣдствіе 5. Сравненіе $x^n + 1 \equiv 0$ (mod. p) имѣетъ d рѣшеній или ни одного, смотря по тому будетъ ли частное $\frac{p-1}{d}$ числомъ четнымъ, или нечетнымъ.

Примѣръ 1. Сравненіе

$$x^{10} \equiv 9 \ (\mathrm{mod.}\ 23)$$

представляетъ намъ случай, когда $d = 2$. Такъ какъ условіе

$$9^{11} \equiv 1 \ (\text{mod. } 23)$$

удовлетворено, то оно имѣетъ два рѣшенія. Далѣе, изъ сравненія

$$5u \equiv 1 \ (\text{mod. } 11)$$

находимъ

$$u = 9, \quad 9^u \equiv 2 \ (\text{mod. } 23);$$

слѣдовательно наше сравненіе приводится къ такому

$$x^2 \equiv 2 \ (\text{mod. } 23).$$

Отсюда находимъ

$$x = 5, \ 18.$$

Примѣръ 2. Сравненіе

$$x^5 \equiv 4 \ (\text{mod. } 19)$$

имѣетъ одно только рѣшеніе. Чтобы найти его, рѣшаемъ сравненіе первой степени

$$5u \equiv 1 \ (\text{mod. } 18);$$

находимъ

$$u = 11;$$

отсюда

$$x \equiv 4^{11} \equiv 16 \ (\text{mod. } 19).$$

ГЛАВА VIII.

Теорія первообразныхъ корней. — Свойства индексовъ.

§ I. О показателяхъ, принадлежащихъ числамъ по данному модулю.

79. Въ виду того, что теоремы, которыя мы намѣрены здѣсь доказывать, одинаково справедливы, какъ при простомъ модулѣ, такъ и при сложномъ, мы будемъ подразумѣвать модуль какимъ угодно.

Пусть a изображаетъ число простое съ модулемъ k. Обозначивъ наименьшіе положительные вычеты степеней

(1). . . . . $a, a^2, a^3, \ldots a^n, \ldots$

соотвѣтственно чрезъ

(2) . . . . $r_1, r_2, r_3, \ldots r_n, \ldots,$

мы замѣчаемъ, что въ ряду (2) нѣтъ нуля; ибо предположеніе $r_n = 0$ приводитъ къ сравненію $a^n \equiv 0 \pmod{k}$, невозможному при a простомъ съ k.

Такъ какъ каждое изъ чиселъ (2) больше нуля и меньше k, то въ числѣ k чиселъ, взятыхъ на удачу изъ (2), всегда найдутся по меньшей мѣрѣ два равныхъ. Положимъ, что $r_j = r_i$, при чемъ $j \leqq k$, $i \leqq k$, $j > i$. Тогда будемъ имѣть

$$a^j \equiv a^i \pmod{k},$$

откуда получаемъ

$$a^{j-i} \equiv 1 \pmod{k}.$$

Это показываетъ, что между первыми $k-1$ числами въ ряду (1) всегда найдется по крайней мѣрѣ одно, которое будетъ сравнимо съ 1.

Доказавъ существованіе одного такого числа, мы непосредственно заключаемъ о существованіи безчисленнаго ихъ множества; ибо, возвышая обѣ части предыдущаго сравненія въ какую нибудь m-ую степень, получаемъ

$$a^{m(j-i)} \equiv 1 \pmod{p}.$$

Между всѣми подобными числами въ (1) особеннаго вниманія заслуживаетъ то, которое стоитъ ближе всего къ началу, или, другими словами, въ выраженіи котораго показатель n наименьшій. Этотъ-то показатель мы будемъ называть *принадлежащимъ числу* a; можно говорить иначе, что a *принадлежитъ къ показателю* n.

Ясно, что сравнимымъ числамъ принадлежатъ равные показатели; но и несравнимымъ числамъ могутъ принадлежать одинакіе показатели. Такъ, напримѣръ, для $k=10$ имѣемъ слѣдующую таблицу показателей:

$$a = 1,\ 3,\ 7,\ 9$$

$$n = 1,\ 4,\ 4,\ 2;$$

отсюда видно, что числа 3 и 7 принадлежатъ къ одному и тому же показателю 4.

80. **Теорема 1.** *Чтобъ имѣло мѣсто сравненіе*

$$a^m \equiv a^{m'} \pmod{k},$$

необходимо и достаточно условіе

$$m \equiv m' \pmod{n},$$

гдѣ n *есть показатель, принадлежащій числу* a.

Докажемъ прежде всего справедливость теоремы въ частномъ случаѣ, когда $m' = 0$.

Обозначивъ частное отъ дѣленія m на n чрезъ q, а остатокъ чрезъ r, имѣемъ $m = nq + r$. Сравненіе

$$a^m \equiv 1 \pmod{k}$$

можно написать такъ:

$$a^{nq} a^r \equiv 1 \pmod{k},$$

или

$$a^r \equiv 1 \pmod{k}.$$

Такъ какъ $r < n$, то изъ послѣдняго сравненія заключаемъ, что r равно нулю. Слѣдовательно $m = nq$, или $m \equiv 0 \pmod{n}$.

Обратно, если $m = nq$, тогда имѣемъ

$$a^m = a^{nq} \equiv 1 \pmod{k},$$

или

$$a^m \equiv a^0 \pmod{k}.$$

Итакъ, въ случаѣ $m' = 0$ справедливость теоремы доказана.

Переходя теперь къ общему случаю, мы представимъ сравненіе

$$(1) \ldots\ldots\ldots\ldots \quad a^m \equiv a^{m'} \pmod{k}$$

такъ:

$$a^{m-m'} \equiv 1 \pmod{k},$$

при чемъ, само собой разумѣется, предполагаемъ $m \geq m'$. Но на основаніи вышедоказаннаго заключаемъ, что послѣднее сравненіе равносильно сравненію $m - m' \equiv 0 \pmod{n}$. Слѣдовательно сравненіе (1) также равносильно сравненію

$$m \equiv m' \pmod{n},$$

что и слѣдовало доказать.

Слѣдствіе 1. *Если a по модулю k принадлежитъ къ показателю n, то всѣ числа въ ряду*

$$1,\ a,\ a^2, \ldots a^{n-1}$$

несравнимы между собой по тому же модулю k.

Ибо числа $0, 1, 2, \ldots n-1$ несравнимы между собой по модулю n.

Слѣдствіе 2. *Если согласимся разсматривать числа сравнимыя по модулю k, какъ будто равныя, то можно сказать, что числа въ ряду*

$$1,\ a,\ a^2, \ldots a^{n-1}, \ldots$$

повторяются періодически, что періодъ состоитъ ровно изъ n различныхъ членовъ и начинается съ перваго члена.

Слѣдствіе 3. *Если число a удовлетворяетъ одновременно двумъ сравненіямъ*

$$a^m \equiv 1,\ a^{m'} \equiv 1 \ (\text{mod.}\ k),$$

то оно удовлетворяетъ и третьему сравненію:

$$a^d \equiv 1 \ (\text{mod.}\ k),$$

гдѣ d изображаетъ общій наибольшій дѣлитель чиселъ m и m'.

Ибо n должно дѣлить оба числа m и m'; поэтому оно должно дѣлить и d.

Теорема 2. *Каково бы ни было число a, показатель, принадлежащій ему по модулю k, есть всегда дѣлитель числа $\varphi(k)$.*

Такъ какъ наименьшіе положительные вычеты чиселъ

$$(2) \ldots\ldots\ldots\ldots 1,\ a,\ a^2, \ldots a^{n-1}$$

суть различные, простые съ k и $< k$, то очевидно имѣемъ $n \leqq \varphi(k)$.

Если $n = \varphi(k)$, справедливость теоремы очевидна.

Допустимъ, что $n < \varphi(k)$. Тогда между числами простыми съ k и $< k$ найдется такое, которое не будетъ сравнимо ни съ

однимъ изъ чиселъ (2). Обозначивъ его чрезъ b, мы замѣчаемъ, что всѣ числа, содержащіяся въ двухъ рядахъ

$$(3)\ldots\ldots\ldots\ldots \begin{cases} 1, a, a^2, \ldots a^{n-1} \\ b, ab, a^2b, \ldots a^{n-1}b \end{cases}$$

несравнимы между собой по модулю k.

На самомъ дѣлѣ, такъ какъ числа въ первой строкѣ (3) несравнимы между собой, то отсюда прямо заключаемъ, что и числа во второй строкѣ (3) несравнимы между собой. Остается показать, что два числа изъ разныхъ строкъ (3) несравнимы. Допустимъ сравненіе вида

$$(4)\ldots\ldots\ldots\ldots a^i b \equiv a^j \pmod{k}.$$

Отсюда, умножая обѣ части на a^{n-i}, выводимъ

$$b \equiv a^{n+j-i} \pmod{k}.$$

Это показываетъ, что b сравнимо съ однимъ изъ чиселъ 1, $a, \ldots a^{n-1}$, другими словами, что b равно наименьшему положительному вычету одного изъ чиселъ 1, a, $a^2, \ldots a^{n-1}$, что противорѣчитъ предположенію; слѣдовательно сравненіе (4) невозможно.

Итакъ, наименьшіе положительные вычеты чиселъ (3) не только простые съ k, что очевидно, но также всѣ различные. Отсюда слѣдуетъ одно изъ двухъ: или $\varphi(k) = 2n$, или $\varphi(k) > 2n$.

Въ первомъ случаѣ справедливость теоремы очевидна, во второмъ — найдется нѣкоторое число c, простое съ k, меньше k и не сравнимое по модулю k ни съ однимъ изъ чиселъ (3).

Возьмемъ во вниманіе систему чиселъ

$$(5)\ldots\ldots\ldots\ldots \begin{cases} 1, a, a^2, \ldots a^{n-1}, \\ b, ab, a^2b, \ldots a^{n-1}b, \\ c, ac, a^2c, \ldots a^{n-1}c. \end{cases}$$

Всѣ они несравнимы между собой по модулю k. Ибо допустивъ, напримѣръ,

$$a^i c \equiv a^j b \pmod{k},$$

выводимъ

$$c \equiv a^{n-i+j} b \pmod{k};$$

отсюда, называя чрезъ r наименьшій положительный вычетъ числа $n - i + j$ по модулю n, получаемъ

$$c \equiv a^r b \pmod{k},$$

что противорѣчитъ предположенію.

Но изъ того, что всѣ числа (5) несравнимы между собой слѣдуетъ заключеніе, что

$$\varphi(k) \geqq 3n.$$

Въ случаѣ, если $\varphi(k)$ окажется $> 3n$, мы будемъ разсуждать далѣе подобно предыдущему, пока не дойдемъ до уравненія вида

$$\varphi(k) = mn,$$

гдѣ m цѣлое число. Такъ справедливость теоремы становится очевидной.

Слѣдствіе. *Если число a простое съ k, то*

$$a^{\varphi(k)} \equiv 1 \pmod{k},$$

каково бы ни было a.

Дѣйствительно, изображая чрезъ n показатель, принадлежащій числу a по модулю k, мы имѣемъ уравненіе $\varphi(k) = nm$, на основаніи котораго заключаемъ

$$a^{\varphi(k)} = (a^n)^m \equiv 1 \pmod{k}.$$

Такъ получается новое доказательство теоремы Эйлера или Фермата.

81. Зная показатель, принадлежащій числу a по данному модулю k, легко опредѣлить показатель, принадлежащій какой

угодно степени a^m по тому же модулю k. Это показываетъ слѣдующая теорема.

Теорема 1. *Если a принадлежитъ къ показателю n по модулю k, то степень a^m, по тому же модулю, принадлежитъ къ показателю $\frac{n}{d}$, при чемъ d изображаетъ общій наибольшій дѣлитель чиселъ m и n.*

Дѣйствительно, обозначивъ чрезъ x показатель, принадлежащій числу a^m, мы замѣчаемъ, что x должно удовлетворять сравненію

(1) . . . . $a^{mx} \equiv 1 \pmod{k}$,

откуда выводимъ

$$mx \equiv 0 \pmod{n}$$

или

$$\frac{m}{d}x \equiv 0 \left(\text{mod. } \frac{n}{d}\right).$$

Рѣшенія этого сравненія получаются изъ формулы

(2) . . . . $t\frac{n}{d}$,

если будемъ полагать послѣдовательно $t = 0, \pm 1, \pm 2, \ldots$; между ними слѣдуетъ искать x. Самое малое по возможности между всѣми положительными числами (2) будетъ искомымъ. Это число есть $\frac{n}{d}$; оно очевидно удовлетворяетъ условію (1), ибо

$$a^{m\frac{n}{d}} = (a^n)^{\frac{m}{d}} \equiv 1 \pmod{k};$$

слѣдовательно

$$x = \frac{n}{d}.$$

Что и слѣдовало доказать.

Слѣдствіе 1. *Если m простое съ n, то a^m принадлежитъ также къ показателю n, какъ и число a.*

Слѣдствіе 2. *Число чиселъ, принадлежащихъ по модулю k къ показателю n, не можетъ быть одновременно меньше $\varphi(n)$ и больше нуля.*

Дѣйствительно, если существуетъ хоть одно число a, принадлежащее къ показателю n по модулю k, то тогда всѣ числа въ ряду

$$a,\ a^2,\ a^3, \ldots a^n,$$

коихъ показатели суть простые съ n, принадлежатъ также къ показателю n по тому же модулю k. Слѣдовательно число такихъ чиселъ не меньше $\varphi(n)$.

Слѣдствіе 3. *Если a принадлежитъ къ показателю n, то можно найти число, которое будетъ принадлежать къ любому дѣлителю d числа n.*

Это число есть $a^{\frac{n}{d}}$.

Теорема 2. *Если a и a' принадлежитъ къ показателямъ n и n', простымъ между собою, то произведеніе aa' принадлежитъ къ показателю nn'.*

Дѣйствительно, обозначивъ чрезъ x показатель, принадлежащій произведенію aa', имѣемъ

(3) . . . . $a^x a'^x \equiv 1 \pmod{k}$.

Отсюда, возвышая обѣ части разъ въ степень n, другой разъ въ n', получаемъ

$$\left.\begin{array}{l} a^{nx}\, a'^{nx} \equiv 1 \\ a^{n'x}\, a'^{n'x} \equiv 1 \end{array}\right\} \pmod{k}.$$

Замѣчая, что $a^n \equiv 1$, $a'^{n'} \equiv 1 \pmod{k}$, послѣднія сравненія можно написать проще такъ:

$$\left.\begin{array}{l} a'^{nx} \equiv 1 \\ a^{n'x} \equiv 1 \end{array}\right\} \pmod{k},$$

откуда вытекаетъ

$$nx \equiv 0 \pmod{n'}$$

$$n'x \equiv 0 \pmod{n}.$$

Сокращая эти сравненія соотвѣтственно на n и на n', получаемъ

$$x \equiv 0 \pmod{n'},$$

$$x \equiv 0 \pmod{n}.$$

Это приводитъ къ заключенію, что x дѣлится на произведеніе nn'.

Полагая

$$x = nn't,$$

намъ остается опредѣлить неизвѣстное t; оно опредѣлится изъ условія (3), которое теперь принимаетъ видъ

$$\textbf{(4)} \ldots\ldots\ldots\ldots a^{nn't} a'^{nn't} \equiv 1 \pmod{k},$$

при чемъ число t должно быть по возможности самымъ малымъ.

Но сравненію (4) удовлетворяетъ очевидно всякое значеніе t, ибо

$$a^{nn't} = (a^n)^{n't} \equiv 1 \pmod{k},$$

$$a'^{nn't} = (a'^{n'})^{nt} \equiv 1 \pmod{k};$$

слѣдовательно $t = 1$, вслѣдствіе чего $x = nn'$. Что и слѣдовало доказать.

Слѣдствіе. *Если нѣсколько чиселъ a, a', a'', . . . принадлежитъ къ показателямъ n, n', n'', . . ., простымъ между собою, то произведеніе $aa'a''$ . . . принадлежитъ къ показателю $nn'n''$. . .*

Послѣднюю теорему можно обобщить слѣдующимъ образомъ.

Теорема 3. *Если a и a' принадлежатъ къ показателямъ n и n', то можно найти число, которое будетъ принадлежать къ показателю, равному наименьшему кратному n и n'.*

На самомъ дѣлѣ, разложивъ наименьшее кратное M чиселъ n и n' на произведеніе простыхъ множителей

$$M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

мы согласимся распредѣлять степени $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots p_r^{\alpha_r}$ на два рода, смотря по тому, которыя изъ нихъ дѣлятъ n и которыя не дѣлятъ n; впрочемъ, тѣ степени, которыя дѣлятъ одновременно и n и n' можно считать безразлично, какъ перваго или какъ втораго рода. Обозначивъ чрезъ λ произведеніе степеней перваго рода, чрезъ μ — втораго, имѣемъ

$$M = \lambda\mu,$$

при чемъ замѣчаемъ: 1) λ и μ суть относительно простыя, 2) λ дѣлитъ n, 3) μ дѣлитъ n'.

Полагая

$$n = \lambda\lambda', \quad n' = \mu\mu'$$

мы заключаемъ, на основаніи одной изъ предыдущихъ теоремъ, что степени

$$a^{\lambda'} \quad \text{и} \quad a'^{\mu'}$$

принадлежатъ соотвѣтственно къ показателямъ

$$\frac{n}{\lambda'} = \lambda, \quad \frac{n'}{\mu'} = \mu;$$

а такъ какъ λ и μ относительно простыя, то произведеніе

$$a^{\lambda'} a'^{\mu'}$$

принадлежитъ къ показателю

$$\lambda\mu = M.$$

Что и слѣдовало доказать.

Слѣдствіе. *Съ помощью чиселъ $a, a', a'', \ldots$ принадлежащихъ соотвѣтственно показателямъ $n, n', n'', \ldots$, можно найти число, которое будетъ принадлежать къ показателю, равному наименьшему кратному чиселъ $n, n', n'' \ldots$*

82. Между различными показателями, соотвѣтствующими всевозможнымъ числамъ простымъ относительно модуля k, осо-

беннаго вниманія заслуживаетъ наибольшій; мы будемъ называть его *наибольшимъ показателемъ по модулю* k, и докажемъ относительно его слѣдующую теорему.

Теорема. *Наибольшій показатель по данному модулю дѣлится на всѣ прочіе показатели.*

Дѣйствительно, положимъ, что a принадлежитъ къ наибольшему показателю m, а b — къ какому нибудь показателю n, отличному отъ m. Еслибы число n не дѣлило m, то наименьшее кратное чиселъ n и m превышало бы m, и тогда по предыдущей теоремѣ можно было бы найти число, которое принадлежало бы показателю $> m$, а это противорѣчитъ предположенію. Слѣдовательно n дѣлитъ m.

Слѣдствіе. *Если m есть наибольшій показатель по модулю k, то сравненію*

$$x^m \equiv 1 \pmod{k}$$

удовлетворяетъ всякое число, простое съ k.

Дѣйствительно, каково бы ни было число b, простое съ k, если обозначимъ чрезъ n принадлежащій ему показатель, имѣемъ

$$(1) \ldots\ldots\ldots\ldots\ldots b^n \equiv 1 \pmod{k};$$

полагая

$$m = nn',$$

число n' будетъ цѣлое. Возвышаемъ обѣ части (1) въ степень n'; получаемъ

$$b^m \equiv 1 \pmod{k}.$$

§ II. Случай, когда модуль простой. О первообразныхъ корняхъ простыхъ чиселъ.

83. **Теорема.** *Наибольшій показатель по простому модулю p есть $p - 1$.*

Первое доказательство. Обозначивъ наибольшій показатель по модулю p чрезъ m, мы замѣчаемъ, что m есть дѣлитель числа $\varphi(p) = p - 1$; поэтому $m < p - 1$, или $m = p - 1$.

Съ другой стороны извѣстно, что сравненію

(1) . . . . $x^m \equiv 1 \pmod{p}$

будетъ удовлетворять всякое число, не дѣлящееся на p, вслѣдствіе чего оно имѣетъ ровно $p-1$ рѣшеній и на основаніи теоремы Лежандра степень его не можетъ быть ниже $p-1$. Слѣдовательно $m=p-1$, и теорема доказана.

Второе доказательство. Изображая чрезъ d любой дѣлитель числа $p-1$, мы ставимъ вопросъ: сколько существуетъ чиселъ, принадлежащихъ, по модулю p, къ показателю d, при чемъ, конечно, числа сравнимыя не принимаются за различныя.

Обозначивъ искомое число чрезъ $\psi(d)$, мы прежде всего постараемся доказать, что имѣть мѣсто можетъ только одно изъ двухъ: $\psi(d)=0$ или $\psi(d)=\varphi(d)$.

Допустивъ, что существуетъ число a, принадлежащее къ показателю d, мы замѣчаемъ, что всѣ рѣшенія сравненія

(2) . . . . $x^d \equiv 1 \pmod{p}$

можно выразить чрезъ a, именно:

(3) . . . . $a^0, a, a^2, \ldots a^{d-1}$.

Ибо каждое число (3) удовлетворяетъ очевидно сравненію (2), и всѣ числа (3) несравнимы по модулю p, а сравненіе (2) не можетъ имѣть болѣе чѣмъ d рѣшеній.

Съ другой стороны, всякое число, принадлежащее къ показателю d, удовлетворяетъ сравненію (1); слѣдовательно въ ряду (2) слѣдуетъ искать всѣхъ чиселъ, принадлежащихъ къ показателю d.

Итакъ, число чиселъ, принадлежащихъ къ показателю d, равно числу чиселъ, содержащихся въ (2) и принадлежащихъ къ показателю d.

Принимая теперь въ соображеніе, что степень a^i тогда только принадлежитъ къ показателю d, когда i простое съ d, мы непосредственно заключаемъ, что $\psi(d)=\varphi(d)$.

Еслибы не существовало вовсе числа, принадлежащаго къ показателю d, тогда слѣдовало бы положить $\psi(d) = 0$.

Для $d = 1$ имѣемъ очевидно $\psi(1) = \varphi(1) = 1$.

Принимая теперь во вниманіе всѣ дѣлители числа $p - 1$

$$1, d, d', \ldots p-1,$$

мы замѣчаемъ, что сумма $\psi(1) + \psi(d) + \psi(d') + \ldots + \psi(p-1)$ выражаетъ собою число чиселъ, содержащихся въ ряду $1, 2, \ldots p - 1$; слѣдовательно

$$(4) \ldots \psi(1) + \psi(d) + \psi(d') + \ldots + \psi(p-1) = p - 1.$$

Съ другой стороны, по извѣстному свойству функціи $\varphi(d)$ имѣемъ

$$(5) \ldots \varphi(1) + \varphi(d) + \varphi(d') + \ldots + \varphi(p-1) = p - 1.$$

Вычитая (4) изъ (5), получаемъ

$$(6) \ldots\ldots [\varphi(1) - \psi(1)] + [\varphi(d) - \psi(d)] + \ldots + [\varphi(p-1) - \psi(p-1)] = 0.$$

По вышедоказанному свойству функціи $\psi(d)$, каждый членъ въ первой части (6) или равенъ нулю, или больше нуля; а такъ какъ ихъ сумма равна нулю, то слѣдовательно каждый равенъ нулю, то есть

$$\psi(1) = \varphi(1),$$
$$\psi(d) = \varphi(d),$$
$$\psi(d') = \varphi(d'),$$
$$\ldots\ldots\ldots$$
$$\ldots\ldots\ldots$$
$$\psi(p-1) = \varphi(p-1).$$

Всѣ эти уравненія заключаются въ слѣдующемъ предложеніи.

Каковъ бы ни былъ дѣлитель d числа $p-1$, число чиселъ, принадлежащихъ къ показателю d, всегда равно $\varphi(d)$.

Въ этомъ предложеніи очевидно содержится наша теорема, которая выражаетъ существенную его часть; остальное провѣряется легко.

На самомъ дѣлѣ, если g есть число, принадлежащее къ показателю $p-1$, то числа

$$0, g, g^2, \ldots g^{p-1}$$

представляютъ полную систему несравнимыхъ чиселъ и потому число чиселъ, принадлежащихъ къ какому нибудь дѣлителю d числа $p-1$, равно (n^0 81, т. 1) числу чиселъ въ ряду $1, 2, \ldots p-1$, имѣющихъ съ $p-1$, каждое порознь, общій наибольшій дѣлитель $\frac{p-1}{d}$. Но извѣстно, что это послѣднее число равно $\varphi(d)$.

Число, принадлежащее къ показателю $p-1$, называется *первообразнымъ корнемъ* числа p. Число первообразныхъ корней есть $\varphi(p-1)$; съ помощью одного изъ нихъ получаются непосредственно всѣ остальные.

84. Предположивъ, что ни a, ни b не дѣлятся на p, мы замѣчаемъ, что если $x = \alpha$ удовлетворяетъ сравненію

$$(1) \ldots\ldots\ldots\ldots\ b^x \equiv a \pmod{p},$$

то и всѣ прочія числа, сравнимыя съ α по модулю $p-1$ будутъ также удовлетворять (1); такія рѣшенія не считаются за различныя. Слѣдовательно сравненіе (1) имѣетъ столько рѣшеній, сколько въ ряду $0, 1, \ldots p-2$ находится удовлетворяющихъ ему чиселъ.

Въ частномъ случаѣ, когда b есть первообразный корень числа p, сравненіе (1) представляетъ особый интересъ. Тогда имѣетъ мѣсто слѣдующая теорема.

Теорема. *Если a не дѣлится на p, а g есть первообразный корень p, то сравненіе*

$$g^x \equiv a \pmod{p}$$

имѣетъ одно и только одно рѣшеніе.

Дѣйствительно, такъ какъ наименьшіе положительные вычеты чиселъ $1, g, g^2, \ldots g^{p-2}$ представляютъ перестановку чиселъ $1, 2, 3 \ldots p-1$, то всякое число a, не дѣлящееся на p, сравнимо по модулю p съ однимъ и только съ однимъ изъ чиселъ $1, g, g^2, g^{p-2}$. Другими словами, въ ряду

$$0, 1, 2, \ldots p-2$$

всегда найдется одно число и только одно, которое будетъ удовлетворять сравненію

$$g^x \equiv a \ (\text{mod.}\, p).$$

Что и слѣдовало доказать.

85. Въ заключеніе даемъ здѣсь таблицу наименьшихъ первообразныхъ корней простыхъ чиселъ, не превышающихъ 100.

p	3	5	7	11	13	17	19	23	29	31	37	41	43
g	2	2	3	2	2	3	2	5	2	3	2	6	3

p	47	53	59	61	67	71	73	79	83	89	97
g	5	2	2	2	2	7	5	3	2	3	5

§ III. О первообразныхъ корняхъ вообще. Опредѣленіе первообразныхъ корней сложныхъ чиселъ вида p^{m+1}, или $2p^{m+1}$.

86. Понятіе о первообразныхъ корняхъ распространяется легко и на сложныя числа.

Первообразнымъ корнемъ какого бы то ни было числа k называется число простое съ k и принадлежащее къ показателю $\varphi(k)$ по модулю k. Если случится, что наибольшій показатель по модулю k меньше $\varphi(k)$, тогда число k не будетъ имѣть вовсе первообразнаго корня.

Допустивъ существованіе первообразнаго корня g для даннаго сложнаго числа k, мы можемъ удостовѣриться легко въ справедливости нижеслѣдующихъ теоремъ.

Теорема. *Если число k имѣетъ одинъ первообразный корень, то оно имѣетъ ихъ ровно* $\varphi(\varphi(k))$.

Дѣйствительно, рядъ чиселъ

$$(1) \ldots\ldots\ldots\ldots\ldots g, g^2, g^3, \ldots g^{\varphi(k)},$$

гдѣ g есть первообразный корень числа k, представляетъ полную систему чиселъ несравнимыхъ по модулю k и простыхъ съ k. Поэтому число всѣхъ первообразныхъ корней числа k равняется числу чиселъ содержащихся въ (1) и принадлежащихъ къ показателю $\varphi(k)$. Но, чтобы число вида g^m принадлежало къ показателю $\varphi(k)$, необходимо и достаточно, чтобы m было простымъ съ $\varphi(k)$; слѣдовательно число первообразныхъ корней числа k равно числу чиселъ простыхъ съ $\varphi(k)$ и содержащихся въ ряду

$$1, 2, 3, \ldots \varphi(k),$$

то есть равно $\varphi(\varphi(k))$.

87. Если показательное сравненіе

$$(1) \ldots\ldots\ldots\ldots\ldots b^x \equiv a \pmod{k}$$

имѣетъ рѣшеніе $x = \alpha$, то всякое число, сравнимое съ α по модулю $\varphi(k)$, также будетъ удовлетворять ему. Поэтому рѣшенія сравненія (1), сравнимыя между собой по модулю $\varphi(k)$, не принято считать за различныя.

Въ частномъ случаѣ, когда b есть первообразный корень, имѣемъ теорему.

Теорема. *Если a простое съ k, а g есть первообразный корень k, то сравненіе*

$$g^x \equiv a \pmod{k}$$

имѣетъ одно и только одно рѣшеніе.

Въ самомъ дѣлѣ, такъ какъ рядъ

$$(2) \ldots\ldots\ldots\ldots\ldots g^0, g, g^2, \ldots g^{\varphi(k)-1}$$

представляетъ полную систему чиселъ несравнимыхъ по модулю $\varphi(k)$ и простыхъ съ k, то всякое число a простое съ k сравнимо по модулю k съ однимъ изъ чиселъ (2) и только съ однимъ, а это доказываетъ справедливость нашей теоремы.

88. Переходя теперь къ рѣшенію вопроса о существованіи первообразнаго корня, мы поставимъ самый вопросъ въ такой формѣ: опредѣлить наибольшій показатель по данному сложному модулю k. При этомъ необходимо переходить постепенно отъ одного частнаго случая къ другому.

Въ настоящемъ параграфѣ мы ограничимся разсмотрѣніемъ трехъ слѣдующихъ случаевъ:

1°. $k = p^{m+1}$, $p > 2$;
2°. $k = 2p^{m+1}$, $p > 2$;
3°. $k = 2^{m+1}$,

при чемъ m изображаетъ произвольное цѣлое число, которое можетъ равняться нулю.

Первый случай, $k = p^{m+1}$, $p > 2$. Каковъ бы ни былъ первообразный корень g простаго числа p, онъ, по теоремѣ Эйлера, удовлетворяетъ сравненію

$$g^{p^m(p-1)} \equiv 1 \ (\text{mod.}\, p^{m+1}).$$

Это сравненіе мы напишемъ въ видѣ уравненія

$$(1) \ldots\ldots\ldots\ldots g^{p^m(p-1)} = 1 + p^{m+1} q_m,$$

гдѣ q_m изображаетъ цѣлое число.

Возвысивъ обѣ части (1) въ степень p, получаемъ

$$(2) \ldots\ldots g^{p^{m+1}(p-1)} = 1 + p^{m+2} q_m + p^{m+3} h,$$

гдѣ h изображаетъ цѣлое число. Здѣсь слѣдуетъ замѣтить, что въ одномъ случаѣ, именно когда $m = 0$, $p = 2$, уравненіе (2) можетъ не имѣть мѣста; поэтому-то мы предположили $p > 2$ и рѣшились случай $p = 2$ разсматривать отдѣльно.

Внося въ обѣ части (1) $m+1$ на мѣсто m, имѣемъ

$$(3) \ldots\ldots\ldots g^{p^{m+1}(p-1)} = 1 + p^{m+2} q_{m+1}.$$

Сличая (2) съ (3), находимъ

$$q_{m+1} = q_m + ph,$$

или

$$(4) \ldots\ldots\ldots\ldots q_{m+1} \equiv q_m \pmod{p}.$$

Сравненіе это показываетъ, что числа

$$(5) \ldots\ldots\ldots\ldots q_0, q_1, q_2, q_3, \ldots q_m, \ldots$$

или всѣ дѣлятся на p, или ни одно изъ нихъ не дѣлится на p. Который изъ этихъ случаевъ будетъ имѣть мѣсто, это зависитъ отъ выбора g; и не трудно показать, что если при данномъ g всѣ числа (5) дѣлятся на p, то стоитъ только увеличить g на p, чтобы ни одно изъ нихъ не дѣлилось на p.

Въ самомъ дѣлѣ, полагая

$$g' = g + p$$

и возвышая въ степень $p-1$, находимъ

$$g'^{p-1} = g^{p-1} + (p-1) p g^{p-2} + hp^2,$$

гдѣ h изображаетъ цѣлое число.

Внося во вторую часть послѣдняго уравненія на мѣсто g^{p-1} равное значеніе по формулѣ

$$g^{p-1} = 1 + pq_0,$$

получаемъ

$$(6) \ldots\ldots g'^{p-1} = 1 + p\left(q_0 + (p-1) g^{p-2}\right) + hp^2.$$

Обозначая чрезъ q'_m значеніе, которое принимаетъ q_m соотвѣтственно корню g', имѣемъ

$$(7) \ldots\ldots\ldots\ldots g'^{p-1} = 1 + pq'_0.$$

Изъ (6) и (7) выводимъ

$$q'_0 = q_0 + (p-1)g^{p-2} + hp.$$

А такъ какъ по предположенію q_0 дѣлится на p, то изъ послѣдняго уравненія заключаемъ

(8) . . . . $q'_0 \equiv (p-1)g^{p-2} \pmod{p}$.

Отсюда ясно, что q'_0 не дѣлится на p, а слѣдовательно и всѣ числа въ ряду

$$q'_0, q'_1, q'_2, \ldots q'_m, \ldots$$

не дѣлятся на p.

На основаніи вышеизложеннаго мы теперь вправѣ предположить, что первообразный корень g числа p такъ подобранъ, что q_0 не дѣлится на p, или, другими словами, что сравненіе

$$g^{\varphi(p^{m+1})} \equiv 1 \pmod{p^{m+2}}$$

ни при какомъ m, начиная съ $m=0$, мѣста не имѣетъ.

Принимая это въ соображеніе, не трудно доказать слѣдующую теорему.

Теорема. *Если g есть первообразный корень нечетнаго простаго числа p, и притомъ частное*

$$\frac{g^{p-1}-1}{p} = q$$

не дѣлится на p, то g есть первообразный корень степени p^{m+1}, каково бы ни было m.

При $m=0$ теорема очевидна. Мы допустимъ, что она вѣрна при какомъ нибудь m и докажемъ ея справедливость при значеніи m на единицу больше.

Обозначимъ чрезъ x показатель принадлежащій числу g по модулю p^{m+2}; этотъ показатель долженъ дѣлить $\varphi(p^{m+2})$; поэтому можно положить

(9) . . . . $p^{m+1}(p-1) = xl$,

при чемъ l изображаетъ цѣлое число.

Далѣе, изъ сравненія

$$g^x \equiv 1 \ (\text{mod.}\, p^{m+2}),$$

вытекаетъ

$$g^x \equiv 1 \ (\text{mod.}\, p^{m+1});$$

а такъ какъ по предположенію число g принадлежитъ по модулю p^{m+1} къ показателю $\varphi(p^{m+1})$, то x должно дѣлиться на $\varphi(p^{m+1})$, и потому можно положить

$$(10) \ldots\ldots\ldots\ldots x = p^m(p-1)\,l',$$

при чемъ l' изображаетъ цѣлое число.

Изъ (9) и (10) выводимъ

$$p = ll',$$

на основаніи чего заключаемъ, что имѣетъ мѣсто одно изъ двухъ: или

$$l = p, \quad l' = 1,$$

или

$$l = 1, \quad l' = p.$$

Первое предположеніе даетъ

$$x = p^m(p-1);$$

тогда сравненіе

$$g^x \equiv 1 \ (\text{mod.}\, p^{m+2})$$

принимаетъ видъ

$$g^{p^m(p-1)} \equiv 1 \ (\text{mod.}\, p^{m+2});$$

а это, по предположенію, не имѣетъ мѣста. Слѣдовательно остается заключить,

$$l = 1, \quad l' = p,$$

вслѣдствіе чего находимъ

$$x = p^{m+1}(p-1) = \varphi(p^{m+2}).$$

Что и слѣдовало доказать.

89. *Второй случай*, $k=2p^{m+1}$, $p>2$. Въ этомъ случаѣ, точно также какъ и въ предшествующемъ, наибольшій показатель равенъ $\varphi(k)$, что равносильно существованію первообразныхъ корней.

Доказательство этого не представляетъ никакого затрудненія; оно вытекаетъ изъ вышеизложеннаго, какъ сейчасъ увидимъ.

Теорема. *Если g есть первообразный корень числа p^{m+1}, тогда изъ двухъ чиселъ g и $g+p^{m+1}$ то, которое нечетное, есть первообразный корень числа $2p^{m+1}$.*

Прежде всего замѣтимъ, что такъ какъ g и $g+p^{m+1}$ суть одновременные первообразные корни числа p^{m+1}, которые не принято даже считать за различные, то мы можемъ прямо предположить, что первообразный корень g есть нечетный.

Принимая это во вниманіе, мы обозначимъ чрезъ x показатель принадлежащій числу g по модулю $2p^{m+1}$. Число x будучи дѣлителемъ $\varphi(2p^{m+1})$ даетъ право написать

(1) . . . . $p^m(p-1)=xl$,

гдѣ l изображаетъ цѣлое число.

Съ другой стороны, изъ сравненія

$$g^x\equiv 1 \pmod{2p^{m+1}},$$

вытекаетъ

$$g^x\equiv 1 \pmod{p^{m+1}}.$$

Отсюда слѣдуетъ, что x дѣлится на $\varphi(p^{m+1})$; ибо g по модулю p^{m+1} принадлежитъ къ показателю $\varphi(p^{m+1})$; слѣдовательно

(2) . . . . $x=p^m(p-1)l'$,

гдѣ l' изображаетъ цѣлое число.

Изъ (1) и (2) выводимъ

$$ll'=1.$$

Слѣдовательно

$$l=1,$$

$$x=p^m(p-1)=\varphi(p^{m+1}).$$

Но

$$\varphi(p^{m+1})=\varphi(2p^{m+1}),$$

ибо p нечетное; поэтому можно написать

$$x=\varphi(2p^{m+1}).$$

Это показываетъ, что g есть первообразный корень числа $2p^{m+1}$.

90. *Третій случай*, $k=2^{m+1}$. Если $m=0$, имѣемъ $k=2$. Это число не представляетъ ничего достойнаго вниманія по отношенію къ первообразнымъ корнямъ, но все же слѣдуетъ замѣтить, что оно имѣетъ первообразный корень.

Если $m=1$, имѣемъ $k=4$. Это число имѣетъ одинъ первообразный корень, именно 3.

Если $m>1$, тогда $k \geqq 8$. Въ этомъ случаѣ число $k=2^{m+1}$ не имѣетъ вовсе первообразныхъ корней; это показываетъ слѣдующая теорема.

Теорема. *Если* $m \geqq 2$, *то наибольшій показатель по модулю* $k=2^{m+1}$ *равенъ* $\frac{1}{2}\varphi(k)=2^{m-1}$.

Для доказательства возьмемъ во вниманіе какое нибудь нечетное число a; квадратъ его можно представить такъ:

$$a^2=1+2^3l,$$

гдѣ l изображаетъ цѣлое число.

Возвышая обѣ части въ квадратъ, получаемъ

$$a^{2^2}=1+2^4l_1,$$

гдѣ l_1 изображаетъ число цѣлое.

Возвышая еще разъ въ квадратъ, получаемъ

$$a^{2^3}=1+2^5l_2,$$

гдѣ l_2 изображаетъ цѣлое число.

Продолжая поступать подобнымъ образомъ далѣе, мы приходимъ къ общей формулѣ

$$a^{2^{m-1}} = 1 + 2^{m+1} l_{m-2},$$

которая можетъ быть написана такъ:

(1) . . . . $a^{\frac{1}{2}\varphi(2^{m+1})} \equiv 1 \pmod{2^{m+1}}$,

причемъ слѣдуетъ имѣть въ виду, что $m \geqq 2$.

Сравненіе (1) показываетъ, что наибольшій показатель по модулю $2^{m+1} \geqq 8$ всегда меньше $\varphi(2^{m+1})$; слѣдовательно числа вида 2^{m+1}, начиная съ 8, первообразныхъ корней не имѣютъ.

Остается теперь доказать существованіе числа, принадлежащаго по модулю $2^{m+1} \geqq 8$ къ показателю 2^{m-1}.

Пусть a изображаетъ какое нибудь число вида $8n \pm 3$,

(2). . . . . $a = 8n \pm 3$.

Возвышая a въ квадратъ, находимъ

$$a^2 = 1 + 2^3 l,$$

гдѣ l изображаетъ нечетное число.

Возвышая обѣ части послѣдняго уравненія въ квадратъ, находимъ

$$a^{2^2} = 1 + 2^4 l_1,$$

гдѣ l_1 изображаетъ нечетное число.

Продолжая далѣе дѣйствовать подобнымъ образомъ, приходимъ къ общей формулѣ

(3) . . . . $a^{2^{m-1}} = 1 + 2^{m+1} l_{m-2}$,

гдѣ l_{m-2} изображаетъ нечетное число.

Изъ полученныхъ уравненій ясно видно, что въ ряду чиселъ

$$a^2 - 1,\ a^{2^2} - 1,\ a^{2^3} - 1, \dots a^{2^{m-1}} - 1,$$

первое, которое дѣлится безъ остатка на 2^{m+1} есть

$$a^{2^{m-1}}-1.$$

Слѣдовательно число $a=8n\pm 3$ по модулю 2^{m+1} принадлежитъ къ показателю $2^{m-1}=\frac{1}{2}\varphi(2^{m+1})$.

Такъ теорема наша доказана вполнѣ.

91. **Теорема.** *Если число a есть вида* $8n\pm 3$, *a* $m\geq 2$, *то числа*

$$1,\quad a,\quad a^2,\quad a^3,\ldots\quad a^{2^{m-1}-1}$$

$$-1,\ -a,\ -a^2,\ -a^3,\ldots -a^{2^{m-1}-1}$$

представляютъ полную систему нечетныхъ чиселъ, несравнимыхъ по модулю 2^{m+1}.

Дѣйствительно, что числа, стоящія въ одной строкѣ несравнимы, это прямо есть слѣдствіе того, что a принадлежитъ къ показателю 2^{m-1}. Намъ остается доказать, что числа въ разныхъ строкахъ также несравнимы по модулю 2^{m+1}. Но для этого очевидно достаточно доказать, что -1 не сравнимо ни съ однимъ изъ чиселъ первой строки.

Допустимъ противное,

$$a^i\equiv -1 \pmod{2^{m+1}},$$

причемъ $i<2^{m-1}$. Тогда будемъ имѣть

$$a^i=-1+2^{m+1}l,$$

откуда, возвышая въ квадратъ, получаемъ

$$a^{2i}=1+2^{m+2}l_1,$$

или

$$a^{2i}\equiv 1 \pmod{2^{m+2}}.$$

Сравненіе это показываетъ, что $2i$ дѣлится на $\frac{1}{2}\varphi(2^{m+2})=2^m$ или, проще, i дѣлится на 2^{m-1}. А такъ какъ, по предположенію,

$i < 2^{m-1}$, то остается положить $i = 0$, что приводитъ къ невозможному сравненію

$$1 \equiv -1 \pmod{2^{m+1}}.$$

Итакъ, -1 не находится въ первой строкѣ; этимъ теорема доказана.

92. Если сравненіе съ двумя неизвѣстными

$$(1) \ldots\ldots (-1)^x a^y \equiv b \pmod{2^{m+1}}, \qquad (m \geqq 2),$$

имѣетъ рѣшеніе $x = \alpha$, $y = \beta$, то всякая пара чиселъ α', β', удовлетворяющихъ условіямъ

$$\alpha' \equiv \alpha \pmod{2}, \quad \beta' \equiv \beta \pmod{2^{m-1}}$$

будетъ также составлять рѣшеніе сравненія (1). Такія рѣшенія не считаются за различныя; поэтому число рѣшеній сравненія (1) равно числу паръ (x, y), удовлетворяющихъ (1) и составленныхъ изъ чиселъ

$$x = 0, 1; \; y = 0, 1, 2, \ldots 2^{m-1} - 1.$$

Принимая это въ соображеніе, мы можемъ послѣднюю теорему выразить такъ:

Каково бы ни было нечетное число b, если a есть вида $8n \pm 3$, то сравненіе

$$(-1)^x a^y \equiv b \pmod{2^{m+1}}, \qquad (m \geqq 2),$$

имѣетъ одно и только одно рѣшеніе.

93. Предполагая какъ прежде $2^{m+1} \geqq 8$, и что a есть вида $8n \pm 3$, мы прибавимъ къ предыдущему слѣдующее замѣчаніе.

Оба числа a^n и $-a^n$ принадлежатъ по модулю 2^{m+1} къ одному и тому же показателю $\frac{2^{m-1}}{d}$, гдѣ d есть общій наибольшій дѣлитель чиселъ 2^{m-1} и n. Исключеніе составляетъ частный случай, когда n дѣлится на 2^{m-1}; тогда a^n принадлежитъ къ показателю 1, а $-a^n$ къ показателю 2.

Вслѣдствіе этого заключаемъ:

1°. Чиселъ, принадлежащихъ къ показателю 2, есть три; они слѣдующія:

$$-1,\ a^{2^{m-2}},\ -a^{2^{m-2}}.$$

2°. Чиселъ, принадлежащихъ къ показателю $2^i > 2$, есть $2\varphi(2^i)$. Они получаются изъ формулы

$$\pm a^{r 2^{m-i-1}}$$

если давать для r всѣ нечетныя значенія $< 2^i$.

§ IV. Опредѣленіе наибольшаго показателя по какому угодно модулю.

94. Частные случаи, разобранные въ предыдущемъ параграфѣ, приводятъ къ рѣшенію общаго вопроса объ опредѣленіи наибольшаго показателя по какому угодно модулю. Прежде чѣмъ показать это, мы докажемъ нижеслѣдующія двѣ теоремы.

Теорема 1. *Если какое нибудь число a по двумъ взаимно простымъ модулямъ k и k' принадлежитъ соотвѣтственно къ показателямъ n и n', то по модулю kk' оно будетъ принадлежать къ показателю, равному наименьшему кратному n и n'.*

Дѣйствительно, обозначивъ чрезъ x показатель, принадлежащій числу a по модулю kk', мы имѣемъ

$$a^x \equiv 1 \pmod{kk'},$$

откуда вытекаютъ два сравненія:

$$a^x \equiv 1 \pmod{k}, \quad a^x \equiv 1 \pmod{k'},$$

которыя показываютъ, что x дѣлится какъ на n такъ и на n'. Слѣдовательно x дѣлится на наименьшее кратное N чиселъ n и n'.

Съ другой стороны имѣемъ сравненія

$$a^N \equiv 1 \pmod{k}, \quad a^N \equiv 1 \pmod{k'},$$

откуда заключаемъ

$$a^N \equiv 1 \ (\mathrm{mod.}\ kk'),$$

а это показываетъ, что N дѣлится на x.

Итакъ, каждое изъ чиселъ x, N дѣлится на остальное; слѣдовательно $x = N$, что и слѣдовало доказать.

Теорема 2. *Если по двумъ взаимно простымъ модулямъ k и k' соотвѣтствующіе наибольшіе показатели суть m и m', то наибольшій показатель по модулю kk' равенъ наименьшему кратному m и m'.*

На самомъ дѣлѣ, называя соотвѣтственно чрезъ a и a' числа, принадлежащія по модулю k или k' къ показателю m или m', мы замѣчаемъ, что число b, удовлетворяющее одновременно двумъ сравненіямъ

$$b \equiv a \ (\mathrm{mod.}\ k), \quad b \equiv a' \ (\mathrm{mod.}\ k'),$$

принадлежитъ по модулю kk' къ показателю M, равному наименьшему кратному чиселъ m и m'.

Съ другой стороны, если обозначимъ соотвѣтственно чрезъ N, n, n' показатели, принадлежащіе какому нибудь числу b' по модулямъ kk', k, k', то замѣчаемъ: во первыхъ, что N есть наименьшее кратное чиселъ n и n'; во вторыхъ, что m и m' дѣлятся соотвѣтственно на n и n'. Слѣдовательно M дѣлится на N; отсюда заключаемъ, что M есть наибольшій показатель по модулю kk'.

Слѣдствіе. *Если m, m', m'', ... суть наибольшіе показатели по соотвѣтствующимъ взаимно простымъ модулямъ k, k', k'', ..., то наибольшій показатель по модулю $kk'k''$ ... равенъ наименьшему кратному чиселъ m, m', m'', ...*

Примѣръ. Положимъ $k = 5$, $k' = 7$, и для каждаго изъ этихъ модулей составимъ таблицу показателей всѣхъ чиселъ.

1°. Для $k = 5$ имѣемъ

$$\text{числа } a = 1,\ 2,\ 3,\ 4;$$

$$\text{показатели } n = 1,\ 4,\ 4,\ 2,$$

2° а для $k = 7$,

$$\text{числа } a' = 1,\ 2,\ 3,\ 4,\ 5,\ 6;$$

$$\text{показатели } n' = 1,\ 3,\ 6,\ 3,\ 6,\ 2.$$

Наибольшій показатель по модулю $kk^{\iota} = 35$ равенъ наименьшему кратному 4 и 6, то есть 12.

Число 3 принадлежитъ къ наибольшему показателю какъ по модулю 5, такъ и по модулю 7; поэтому по модулю 35 оно принадлежитъ къ показателю 12, также наибольшему.

Число 2 принадлежитъ къ показателю 4, по модулю 5, а по модулю 7 къ показателю 3; наименьшее кратное 4 и 3 есть 12; слѣдовательно 2 по модулю 35 принадлежитъ къ показателю 12.

Число 4 по модулямъ 5 и 7 принадлежитъ соотвѣтственно къ показателямъ 2 и 3; наименьшее кратное этихъ чиселъ есть 6; слѣдовательно 4 по модулю 35 принадлежитъ къ показателю 6.

95. **Теорема.** *Каково бы ни было число*

$$k = 2^n p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

наибольшій показатель по модулю k равенъ одному изъ двухъ: или наименьшему кратному чиселъ

$$\varphi(2^n),\ \varphi(p_1^{\alpha_1}),\ \varphi(p_2^{\alpha_2}), \ldots \varphi(p_r^{\alpha_r}),$$

или наименьшему кратному чиселъ

$$\tfrac{1}{2}\varphi(2^n),\ \varphi(p_1^{\alpha_1}),\ \varphi(p_2^{\alpha_2}), \ldots \varphi(p_r^{\alpha_r}).$$

Первый случай имѣетъ мѣсто, когда $n \leqq 2$, второй — когда $n > 2$.

Дѣйствительно, полагая

$$k_1 = 2^n,\ k_2 = p_1^{\alpha_1}, \ldots k_{r+1} = p_r^{\alpha_r},$$

мы замѣчаемъ, что числа $k_1, k_2, \ldots k_{r+1}$ суть взаимно простыя. Обозначая соотвѣтственно чрезъ $m_1, m_2, \ldots m_{r+1}$ наибольшіе

показатели по модулямъ $k_1, k_2, \ldots k_{r+1}$, имѣемъ: во первыхъ, $m_1 = \varphi(2^n)$ или $m_1 = \frac{1}{2}\varphi(2^n)$, смотря по тому будетъ ли $n \leq 2$ или $n > 2$; во вторыхъ, $m_2 = \varphi(p_1^{\alpha_1})$, $m_3 = \varphi(p_2^{\alpha_2}), \ldots$ $m_{r+1} = \varphi(p_r^{\alpha_r})$. Отсюда, на основаніи теоремы n^0 94 заключаемъ, что наибольшій показатель по модулю $k = k_1 k_2 \ldots k_{r+1}$ равенъ наименьшему кратному чиселъ $m_1, m_2, \ldots m_{r+1}$; а это и составляетъ сущность предложенной теоремы.

Число k только тогда имѣетъ первообразный корень, когда соотвѣтствующій ему, какъ модулю, наибольшій показатель равенъ $\varphi(k)$. Но это имѣетъ мѣсто только въ слѣдующихъ четырехъ случаяхъ:

$$k = 2,\ 4,\ p^\alpha,\ 2p^\alpha.$$

Всѣ эти случаи были разобраны въ предшествующемъ параграфѣ.

96. Рѣшенія сравненія

(1). . . . . $f(x) \equiv 0 \pmod{k}$

при сложномъ модулѣ слѣдуетъ раздѣлять на два рода: простыя съ k, и имѣющія съ k общій дѣлитель.

Если дѣло идетъ объ отысканіи рѣшеній исключительно перваго рода, то тогда степень сравненія можно понизить на столько, чтобы она была ниже наибольшаго показателя n, соотвѣтствующаго модулю k. Для этого стоитъ только функцію $f(x)$ раздѣлить на $x^n - 1$. Остатокъ $f_1(x)$, полученный отъ этого дѣленія, будетъ степени ниже n, и сравненіе

(2) . . . . $f_1(x) \equiv 0 \pmod{k}$

будетъ имѣть всѣ рѣшенія перваго рода общими съ (1).

Примѣръ. Возьмемъ во вниманіе сравненіе

$$x^5 - 7x^4 + 11x^3 - 5x + 1 \equiv 0 \pmod{12}.$$

Такъ какъ послѣдній членъ въ первой части простой относительно 12, то сравненіе не имѣетъ вовсе рѣшеній втораго рода.

Наибольшій показатель по модулю 12, будучи равнымъ наименьшему кратному чиселъ $\varphi(4)$ и $\varphi(3)$, есть 2; поэтому всякое число простое съ 12 удовлетворяетъ сравненію

$$x^2 \equiv 1 \pmod{12}.$$

Отсюда выводимъ

$$x^3 \equiv x,\ x^4 \equiv 1,\ x^5 \equiv x \pmod{12},$$

вслѣдствіе чего начальное сравненіе приводится къ такому

$$x - 7 + 11x - 5x + 1 \equiv 0 \pmod{12},$$

или

$$7x - 6 \equiv 0 \pmod{12}.$$

Сравненіе это не имѣетъ ни одного рѣшенія простаго относительно 12; поэтому начальное сравненіе невозможно.

§ V. Новое доказательство теоремы Вильсона въ обобщенной формѣ.

97. **Лемма.** *Если g есть первообразный корень числа $k > 2$, то*

$$g^{\frac{1}{2}\varphi(k)} \equiv -1 \pmod{k}.$$

Лемма эта вытекаетъ непосредственно изъ теоремы 2-ой n^0 67; однако, имѣя въ виду пользоваться здѣсь исключительно началами теоріи первообразныхъ корней, мы дадимъ другое ея доказательство.

Въ случаѣ $k = 4$ справедливость леммы провѣряется непосредственно.

Въ случаѣ $k = p^\alpha$ мы замѣчаемъ, что число $\varphi(k)$ четное; поэтому сравненіе

$$g^{\varphi(k)} - 1 \equiv 0 \pmod{p^\alpha}$$

можетъ быть написано такъ:

(1). . . . . . $(g^{\frac{1}{2}\varphi(k)} - 1)(g^{\frac{1}{2}\varphi(k)} + 1) \equiv 0 \pmod{p^\alpha}$.

Не можетъ быть, чтобъ оба множителя въ первой части дѣлились на p, потому что тогда мы имѣли бы два сравненія

$$\left.\begin{array}{l} g^{\frac{1}{2}\varphi(k)} - 1 \equiv 0 \\ g^{\frac{1}{2}\varphi(k)} + 1 \equiv 0 \end{array}\right\} (\text{mod. } p),$$

откуда вытекаетъ

$$2 \equiv 0 \ (\text{mod. } p);$$

а это невозможно, ибо p подразумѣвается нечетнымъ простымъ числомъ.

Итакъ, одинъ изъ множителей (1) есть простой относительно p^{α}; слѣдовательно одинъ изъ нихъ дѣлится на p^{α}. Но первый множитель, именно

$$g^{\frac{1}{2}\varphi(k)} - 1$$

не можетъ дѣлиться на p^{α}; иначе g не было бы первообразнымъ корнемъ числа k; слѣдовательно

$$g^{\frac{1}{2}\varphi(k)} \equiv -1 \ (\text{mod. } p^{\alpha}).$$

Остается еще показать справедливость леммы въ случаѣ $k = 2p^{\alpha}$. Тогда число $\varphi(k)$ есть четное, g — нечетное, и мы опять имѣемъ сравненіе (1), въ первой части котораго оба множителя суть четные. Одинъ изъ нихъ простой относительно p^{α}, другой дѣлится на p^{α}, а тѣмъ самымъ дѣлится и на $2p^{\alpha}$. Но множитель $g^{\frac{1}{2}\varphi(k)} - 1$ не дѣлится на $2p^{\alpha}$; иначе g не было бы первообразнымъ корнемъ числа $2p^{\alpha}$; слѣдовательно

$$g^{\frac{1}{2}\varphi(k)} + 1 \equiv 0 \ (\text{mod. } 2p^{\alpha}).$$

Что и требовалось доказать.

98. Переходимъ теперь къ доказательству обобщенной теоремы Вильсона.

Теорема. *Абсолютно малый вычетъ произведенія всѣхъ чиселъ, простыхъ съ модулемъ k и $< k$, равенъ -1 или $+1$, смотря по тому имѣетъ ли число k первообразный корень или нѣтъ.*

Предположимъ сперва, что k имѣетъ первообразный корень; другими словами, что имѣетъ мѣсто одинъ изъ четырехъ случаевъ: $k = 2,\ 4,\ p^\alpha,\ 2p^\alpha$.

Въ двухъ первыхъ случаяхъ справедливость теоремы провѣряется непосредственно.

Въ двухъ послѣднихъ случаяхъ мы замѣчаемъ, что совокупность наименьшихъ положительныхъ вычетовъ чиселъ

$$g^0 = 1,\ g,\ g^2, \ldots g^{\varphi(k)-1},$$

гдѣ g изображаетъ первообразный корень k, — представляетъ всѣ числа простыя съ k и $< k$. Поэтому, изображая ихъ произведеніе чрезъ Π, имѣемъ сравненіе

$$\Pi \equiv g^{1+2+3+\ldots+\varphi(k)-1} \ (\text{mod. } k),$$

которое можно написать такъ:

$$\Pi \equiv g^{\frac{\varphi(k)}{2}\left(\varphi(k)-1\right)} \ (\text{mod. } k).$$

Но по вышедоказанному имѣемъ

$$g^{\frac{\varphi(k)}{2}} \equiv -1 \ (\text{mod. } p);$$

слѣдовательно

$$\Pi \equiv (-1)^{\varphi(k)-1} \ (\text{mod. } k).$$

А такъ какъ число $\varphi(k)$ всегда четное, то послѣднее сравненіе можно написать такъ:

$$\Pi \equiv -1 \ (\text{mod. } k).$$

Остается теперь доказать справедливость теоремы въ предположеніи, что k не имѣетъ первообразнаго корня.

Допустимъ сначала

$$k = 2^n, \quad n > 2.$$

Тогда по теоремѣ n^0 91 имѣемъ

$$\Pi \equiv (-1)^{2^{n-2}} 3^{2(1+2+3+\ldots+2^{n-2}-1)} \pmod{2^n}$$

или, проще,

$$\Pi \equiv 3^{2^{n-2}(2^{n-2}-1)} \pmod{2^n}.$$

А такъ какъ число 3 по модулю 2^n принадлежитъ къ показателю $\frac{1}{2}\varphi(2^n) = 2^{n-2}$, то

$$3^{2^{n-2}} \equiv 1 \pmod{2^n},$$

вслѣдствіе чего предыдущее сравненіе принимаетъ видъ

$$\Pi \equiv 1 \pmod{2^n};$$

что подтверждаетъ справедливость теоремы въ предположенномъ случаѣ.

Переходя теперь къ общему случаю

$$k = 2^n p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

мы возьмемъ во вниманіе всѣ числа

$$1, a_1, a_2, \ldots a_{\varphi(k)-1}$$

простыя съ k и $< k$, и назовемъ ихъ наименьшіе положительные вычеты по модулю $p_i^{\alpha_i}$ чрезъ

$$1, r_1^{(i)}, r_2^{(i)}, \ldots r_{\varphi(k)-1}^{(i)}.$$

Послѣдній рядъ содержитъ всѣ числа простыя съ p_i и $< p_i^{\alpha_i}$, при томъ каждое число повторяется въ немъ ровно

$$\varphi(2^n)\,\varphi(p_1^{\alpha_1}) \ldots \varphi(p_{i-1}^{\alpha_{i-1}})\,\varphi(p_{i+1}^{\alpha_{i+1}}) \ldots \varphi(p_r^{\alpha_r})$$

разъ. Слѣдовательно, изображая чрезъ P_i произведеніе всѣхъ чиселъ простыхъ съ p_i и $< p_i^{\alpha_i}$, имѣемъ

$$\Pi \equiv P^{\varphi(2^n) \ldots \varphi(p_{i-1}^{\alpha_{i-1}})\,\varphi(p_{i+1}^{\alpha_{i+1}}) \ldots \varphi(p_r^{\alpha_r})} \pmod{p_i^{\alpha_i}}.$$

Но по вышедоказанному имѣемъ

$$P \equiv -1 \ (\text{mod.}\ p_i^{\alpha});$$

слѣдовательно

$$\Pi \equiv 1 \ (\text{mod.}\ p_i^{\alpha_i});$$

ибо показатель надъ буквою P въ предыдущемъ сравненіи очевидно четный.

Въ послѣднемъ сравненіи значекъ i можетъ принимать любое изъ значеній

$$i = 1,\ 2,\ 3, \ldots r;$$

поэтому можемъ написать

$$(1) \ldots\ldots\ldots\ldots \begin{cases} \Pi \equiv 1 \ (\text{mod.}\ p_1^{\alpha_1}), \\ \Pi \equiv 1 \ (\text{mod.}\ p_2^{\alpha_2}), \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ \Pi \equiv 1 \ (\text{mod.}\ p_r^{\alpha_r}). \end{cases}$$

Сверхъ того по вышедоказанному имѣемъ

$$(2) \ldots\ldots\ldots\ldots \Pi \equiv 1 \ (\text{mod.}\ 2^n).$$

Изъ (1) и (2) заключаемъ

$$\Pi \equiv 1 \ (\text{mod.}\ 2^n p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r})$$

или

$$\Pi \equiv 1 \ (\text{mod.}\ k).$$

Что и слѣдовало доказать.

§ VI. Теорія индексовъ. Приложенія.

99. Извѣстно, что если число k имѣетъ первообразный корень g, то всякое число a простое съ k можно представить такъ:

$$(1) \ldots\ldots\ldots\ldots a \equiv g^x \ (\text{mod.}\ k),$$

гдѣ x изображаетъ нѣкоторое изъ чиселъ

(2) . . . . $0, 1, 2, \ldots \varphi(k)-1.$

Кромѣ этого одного рѣшенія x сравненіе (1) имѣетъ безчисленное множество другихъ, опредѣляемыхъ по общей формулѣ

$$x + t\varphi(k),$$

гдѣ t изображаетъ произвольное цѣлое число.

Число x, удовлетворяющее (1) и содержащееся въ (2) называется *индексомъ* или *указателемъ* числа a; число g называется *основаніемъ* системы индексовъ.

Индексъ какого нибудь числа a для сокращенія изображается символомъ

$$\operatorname{Ind} a.$$

Онъ обладаетъ свойствами аналогичными со свойствами логариѳмовъ.

Если $a \equiv b \pmod{k}$, то очевидно $\operatorname{Ind} a = \operatorname{Ind} b$.

Индексъ основанія всегда равенъ 1. Сверхъ того имѣемъ $\operatorname{Ind} 1 = 0$, $\operatorname{Ind}(-1) = \frac{1}{2}\varphi(k)$.

100. **Теорема.** *Индексъ произведенія двухъ чиселъ сравнимъ по модулю $\varphi(k)$ съ суммой ихъ индексовъ.*

Дѣйствительно, мы имѣемъ два сравненія

$$a \equiv g^{\operatorname{Ind} a} \pmod{k}$$

$$a' \equiv g^{\operatorname{Ind} a'} \pmod{k},$$

которыя перемножая почленно, получаемъ

$$aa' \equiv g^{\operatorname{Ind} a + \operatorname{Ind} a'} \pmod{k}.$$

Но, съ другой стороны, имѣемъ

$$aa' \equiv g^{\operatorname{Ind} aa'} \pmod{k};$$

слѣдовательно

$$g^{\operatorname{Ind} aa'} \equiv g^{\operatorname{Ind} a + \operatorname{Ind} a'} \pmod{k}.$$

А такъ какъ g принадлежитъ къ показателю $\varphi(k)$, то изъ послѣдняго сравненія вытекаетъ

$$\operatorname{Ind} aa' \equiv \operatorname{Ind} a + \operatorname{Ind} a' \pmod{\varphi(k)}.$$

Что и слѣдовало доказать.

Слѣдствіе 1. *Индексъ произведенія какого угодно числа чиселъ сравнимъ по модулю $\varphi(k)$ съ суммой ихъ индексовъ.*

Слѣдствіе 2. *Индексъ степени какого угодно числа сравнимъ по модулю $\varphi(k)$ съ произведеніемъ показателя степени на индексъ числа.*

Отсюда слѣдуетъ, что по даннымъ индексамъ чиселъ a, a', a'', . . . легко вычислить индексъ произведенія $aa'a''$ . . . Для этого стоитъ только составить наименьшій положительный вычетъ суммы $\operatorname{Ind} a + \operatorname{Ind} a' + \operatorname{Ind} a'' + \ldots$ по модулю $\varphi(k)$; это и будетъ искомый индексъ.

Наименьшій положительный вычетъ произведенія $n \operatorname{Ind} a$ равенъ индексу степени a^n.

101. Имѣя таблицы индексовъ всѣхъ чиселъ, составленныя для различныхъ модулей, можемъ ими пользоваться для удобнаго рѣшенія разныхъ вопросовъ въ теоріи чиселъ, подобно тому какъ въ алгебрѣ пользуются логариѳмическими таблицами.

Возьмемъ во вниманіе сравненіе

$$(1) \ldots\ldots\ldots\ldots\ldots x^n \equiv q \pmod{k},$$

гдѣ q простое съ k, и положимъ что k имѣетъ первообразный корень g.

Искомое рѣшеніе x должно быть простымъ съ k, а такъ какъ индексы чиселъ сравнимыхъ между собой равны, то

$$\operatorname{Ind} x^n = \operatorname{Ind} q.$$

Съ другой стороны имѣемъ

$$\operatorname{Ind} x^n \equiv n \operatorname{Ind} x \pmod{\varphi(k)};$$

слѣдовательно

$$(2) \ldots\ldots\ldots n \operatorname{Ind} x \equiv \operatorname{Ind} q \pmod{\varphi(k)}.$$

Это сравненіе первой степени относительно неизвѣстнаго $\operatorname{Ind} x$. Если общій наибольшій дѣлитель d чиселъ n и $\varphi(k)$ дѣлитъ $\operatorname{Ind} q$, тогда оно имѣетъ ровно d рѣшеній, несравнимыхъ по модулю $\varphi(k)$. Наименьшій положительный вычетъ каждаго изъ этихъ рѣшеній будетъ индексомъ соотвѣтствующаго рѣшенія сравненія (1). По данному $\operatorname{Ind} x$ мы отыщемъ въ таблицахъ самое число x, и такимъ образомъ можно опредѣлить всѣ d рѣшеній (1).

Если $\operatorname{Ind} q$ не дѣлится на d, тогда (2), а тѣмъ самымъ и (1) невозможно.

Только что полученное условіе, необходимое и достаточное для того, чтобы сравненіе (1) имѣло рѣшеніе, можно выразить въ другой формѣ. Дѣйствительно, по означенному условію можно написать

$$q \equiv g^{dd'} \ (\text{mod. } k);$$

отсюда, возвышая обѣ части въ степень $\frac{\varphi(k)}{d}$, получаемъ

$$(3) \ldots\ldots\ldots\ldots \quad q^{\frac{\varphi(k)}{d}} \equiv 1 \ (\text{mod. } k).$$

Легко доказать обратное: если (3) имѣетъ мѣсто, то тогда (1) возможно. Для этого возвысимъ обѣ части сравненія

$$q \equiv g^{\operatorname{Ind} q} \ (\text{mod. } k)$$

въ степень $\frac{\varphi(k)}{d}$; получаемъ

$$g^{\frac{\varphi(k)}{d} \operatorname{Ind} q} \equiv q^{\frac{\varphi(k)}{d}} \ (\text{mod. } k).$$

Это на основаніи (3) принимаетъ видъ

$$g^{\frac{\varphi(k)}{d} \operatorname{Ind} q} \equiv 1 \ (\text{mod. } k).$$

Отсюда заключаемъ, что показатель

$$\frac{\varphi(k)}{d} \operatorname{Ind} q$$

дѣлится безъ остатка на $\varphi(k)$, другими словами, что $\operatorname{Ind} q$ дѣлится на d. Слѣдовательно сравненіе (1) имѣетъ рѣшеніе, и условіе (3) вполнѣ равносильно прежде найденному. Это даетъ такую теорему (n^0 78).

Теорема. *Если k имѣетъ первообразный корень, то сравненіе*

$$x^n \equiv q \pmod{k}$$

возможно или невозможно, смотря по тому удовлетворено ли условіе

$$q^{\frac{\varphi(k)}{d}} \equiv 1 \pmod{k},$$

или нѣтъ; при чемъ d изображаетъ общій наибольшій дѣлитель n и $\varphi(k)$.

Въ случаѣ, если условіе удовлетворено, сравненіе имѣетъ ровно d рѣшеній.

102. Перейдемъ къ другому частному случаю, именно $k = 2^m \geqq 8$, и разсмотримъ сравненіе

(1) . . . . $x^n \equiv q \pmod{2^m}$,

предполагая, конечно, q числомъ нечетнымъ.

Извѣстно, что всякое нечетное число q можно представить въ видѣ

$$q \equiv (-1)^\alpha\, 3^\beta \pmod{2^m},$$

гдѣ α равно нулю или 1, а β равно одному изъ чиселъ 0, 1, 2,... $2^{m-2}-1$.

Положивъ

$$x \equiv (-1)^\xi\, 3^\eta,$$

вмѣсто (1) будемъ имѣть

$$(-1)^{n\xi}\, 3^{n\eta} \equiv (-1)^\alpha\, 3^\beta \pmod{2^m}.$$

Сравненіе это распадается на два, именно,

$$(2) \ldots\ldots\ldots\ldots \begin{cases} n\xi \equiv \alpha \pmod{2}, \\ n\eta \equiv \beta \pmod{2^{m-2}}; \end{cases}$$

изъ нихъ первое служитъ для опредѣленія ξ, второе — для опредѣленія η.

Если n нечетное, оба сравненія (2) имѣютъ по одному рѣшенію и тогда сравненіе (1) имѣетъ одно рѣшеніе.

Если же n четное, то, чтобы сравненія (2) были возможны, необходимы и достаточны условія:

$$(3) \ldots\ldots\ldots\ldots \alpha = 0$$

$$(4) \ldots\ldots\ldots\ldots \beta \equiv 0 \pmod{d},$$

гдѣ d изображаетъ общій наибольшій дѣлитель чиселъ n и 2^{m-2}.

Допустивъ, что послѣднія условія удовлетворены и положивъ

$$q \equiv 3^{dd'} \pmod{2^m},$$

имѣемъ

$$(5) \ldots\ldots\ldots\ldots q^{\frac{2^{m-2}}{d}} \equiv 1 \pmod{2^m}.$$

Обратно, допустивъ, что (5) имѣетъ мѣсто и положивъ

$$q \equiv (-1)^\alpha \, 3^\beta \pmod{2^m},$$

имѣемъ

$$(-1)^{\alpha \frac{2^{m-2}}{d}} \, 3^{\beta \frac{2^{m-2}}{d}} \equiv 1 \pmod{2^m},$$

откуда заключаемъ

$$\alpha \frac{2^{m-2}}{d} \equiv 0 \pmod{2}$$

$$\beta \frac{2^{m-2}}{d} \equiv 0 \pmod{2^{m-2}}.$$

Послѣднее сравненіе приводится къ слѣдующему виду

$$\beta \equiv 0 \pmod{d},$$

что совпадаетъ съ (4). Слѣдовательно условіе (5) замѣняетъ (4).

Такимъ образомъ мы доказали теорему:

Теорема. *Сравненіе*

$$x^n \equiv q \pmod{2^m}, \quad (m > 2), \quad (q = 2l + 1),$$

при нечетномъ n имѣетъ всегда одно только рѣшеніе.

При четномъ n оно возможно только въ томъ случаѣ, когда удовлетворены два условія: во первыхъ, должно имѣть мѣсто сравненіе

$$q^{\frac{2^{m-2}}{d}} \equiv 1 \pmod{2^m},$$

гдѣ d есть общій наибольшій дѣлитель чиселъ n и 2^{m-2}; во вторыхъ, число q должно быть вида $8t + 1$.

При соблюденіи означенныхъ условій сравненіе имѣетъ ровно $2d$ рѣшеній.

Послѣднія двѣ теоремы даютъ возможность опредѣлить a priori число рѣшеній сравненія

$$x^n \equiv q \pmod{k}$$

при какомъ угодно k.

Примѣръ. Возьмемъ сравненіе

$$x^3 \equiv 125 \pmod{504};$$

оно приводится къ тремъ слѣдующимъ:

$$x^3 \equiv 5 \pmod{8}, \quad x^3 \equiv 6 \pmod{7}, \quad x^3 \equiv 8 \pmod{9}.$$

Соотвѣтствующія имъ условія возможности суть такія:

$$6^2 \equiv 1 \pmod{7}, \quad 8^2 \equiv 1 \pmod{9}.$$

Такъ какъ каждое изъ нихъ въ дѣйствительности удовлетворено, то послѣднія сравненія имѣютъ соотвѣтственно

$$1, \ 3, \ 3$$

рѣшеній. Произведеніе этихъ чиселъ равно 9; поэтому число рѣшеній начальнаго сравненія есть 9.

103. Вышеизложенныя начала теоріи индексовъ можно распространить и на модуль $2^m \geqq 8$; но только тогда каждое число будетъ опредѣляться двумя индексами.

Дѣйствительно, каково бы ни было нечетное число n, мы можемъ положить

$$n \equiv (-1)^\alpha \, 3^\beta \ (\text{mod. } 2^m),$$

причемъ $\alpha = 0$ или 1, смотря по тому будетъ ли число n вида $8t+1$ или $8t+3$, или не будетъ; $\beta < 2^{m-2}$. Показатель α назовемъ первымъ индексомъ числа n по основанію 3, а показатель β — вторымъ, и будемъ писать

$$\alpha = \text{Ind}_1 n, \quad \beta = \text{Ind}_2 n.$$

Тогда легко убѣдиться въ справедливости слѣдующихъ предложеній.

1°. *Какъ первые, такъ и вторые индексы сравнимыхъ чиселъ соотвѣтственно равны между собой.*

2°. *Индексы произведенія нѣсколькихъ чиселъ опредѣляются по формуламъ*

$$\text{Ind}_1 ab \ldots c \equiv \text{Ind}_1 a + \text{Ind}_1 b + \ldots + \text{Ind}_1 c \ (\text{mod. } 2),$$

$$\text{Ind}_2 ab \ldots c \equiv \text{Ind}_2 a + \text{Ind}_2 b + \ldots + \text{Ind}_2 c \ (\text{mod. } 2^{m-2}).$$

3°. *Индексы степени опредѣляются по формуламъ*

$$\text{Ind}_1 a^n \equiv n \, \text{Ind}_1 a \ (\text{mod. } 2),$$

$$\text{Ind}_2 a^n \equiv n \, \text{Ind}_2 a \ (\text{mod. } 2^{m-2}).$$

Имѣя таблицу индексовъ всѣхъ чиселъ по модулю 2^m, можемъ при ея помощи удобно рѣшать сравненія вида

$$(1) \ldots\ldots\ldots\ldots\ldots \; x^n \equiv q \pmod{2^m}.$$

Дѣйствительно, изъ (1) выводимъ

$$(2) \ldots\ldots\ldots \; n\,\mathrm{Ind}_1 x \equiv \mathrm{Ind}_1 q \pmod{2},$$

$$(3) \ldots\ldots\ldots \; n\,\mathrm{Ind}_2 x \equiv \mathrm{Ind}_2 q \pmod{2^{m-2}}.$$

Если n нечетное, оба сравненія (2) и (3) имѣютъ по одному рѣшенію. Рѣшенія эти опредѣляютъ индексы неизвѣстнаго x; по нимъ изъ таблицы отыщемъ прямо x.

Если же n четное, тогда сравненія (2) и (3) возможны только при условіи, чтобы значеніе $\mathrm{Ind}_1 q$ было четное, а $\mathrm{Ind}_2 q$ дѣлилось на общій наибольшій дѣлитель d чиселъ n и 2^{n-2}. Смотря по тому, будетъ ли это двойное условіе удовлетворено или нѣтъ, сравненіе (1) будетъ имѣть $2d$ рѣшеній или ни одного.

Примѣръ. Принимая за модуль число $64 = 2^6$, а за основаніе 3, составимъ двѣ таблицы, изъ которыхъ первая содержитъ индексы всѣхъ чиселъ по порядку, а вторая даетъ возможность по даннымъ двумъ индексамъ опредѣлить прямо соотвѣтствующее число.

n	$\text{Ind}_1 n$	$\text{Ind}_2 n$	$\text{Ind}_1 n$	$\text{Ind}_2 n$	n
1	0	0	0	0	1
3	0	1	0	1	3
5	1	11	0	2	9
7	1	14	0	3	27
9	0	2	0	4	17
11	0	7	0	5	51
13	1	5	0	6	25
15	1	12	0	7	11
17	0	4	0	8	33
19	0	13	0	9	35
21	1	15	0	10	41
23	1	10	0	11	59
25	0	6	0	12	49
27	0	3	0	13	19
29	1	8	0	14	57
31	1	9	0	15	43
33	0	8	1	0	63
35	0	9	1	1	61
37	1	3	1	2	55
39	1	6	1	3	37
41	0	10	1	4	47
43	0	15	1	5	13
45	1	13	1	6	39
47	1	4	1	7	53
49	0	12	1	8	29
51	0	5	1	9	31
53	1	7	1	10	23
55	1	2	1	11	5
57	0	14	1	12	15
59	0	11	1	13	45
61	1	1	1	14	7
63	1	0	1	15	21

При помощи этихъ таблицъ предложимъ себѣ рѣшить сравненіе

$$x^6 \equiv 41 \pmod{64}.$$

Для этого беремъ индексы обѣихъ частей и получаемъ

$$6\,\mathrm{Ind}_1 x \equiv \mathrm{Ind}_1 41 \pmod{2},$$

$$6\,\mathrm{Ind}_2 x \equiv \mathrm{Ind}_2 41 \pmod{16}.$$

Изъ первой таблицы находимъ $\mathrm{Ind}_1 41 = 0$, $\mathrm{Ind}_2 41 = 10$; слѣдовательно имѣемъ

$$6\,\mathrm{Ind}_1 x \equiv 0 \pmod{2},$$

$$6\,\mathrm{Ind}_2 x \equiv 10 \pmod{16},$$

откуда выводимъ

$$\mathrm{Ind}_1 x = 0,\ 1;$$

$$\mathrm{Ind}_2 x = 7,\ 15.$$

Эти значенія даютъ четыре различныхъ рѣшенія для x; всѣ они опредѣляются непосредственно изъ второй таблицы, именно:

$$x = 11,\ 43,\ 53,\ 21.$$

104. Возвращаясь къ тому случаю, когда модуль k имѣетъ первообразный корень, мы обозначимъ чрезъ g и g' два какихъ нибудь первообразныхъ корня числа k и примемъ во вниманіе индексы произвольнаго числа a, взятые разъ по основанію g, другой разъ по основанію g'; первый изъ нихъ будемъ изображать чрезъ $\mathrm{Ind}_g a$, второй чрезъ $\mathrm{Ind}_{g'} a$.

Положивъ это, мы замѣчаемъ, что рѣшеніе сравненія

$$g'^x \equiv a \pmod{k}$$

можно выразить такъ:

$$x = \mathrm{Ind}_{g'} a.$$

Съ другой стороны, взявъ индексы обѣихъ частей предыдущаго сравненія по основанію g, получаемъ

$$x \operatorname{Ind}_g g' \equiv \operatorname{Ind}_g a \pmod{\varphi(k)}.$$

Отсюда, внося на мѣсто x предыдущее выраженіе, получаемъ

$$(1) \ldots\ldots \operatorname{Ind}_{g'} a \operatorname{Ind}_g g' \equiv \operatorname{Ind}_g a \pmod{\varphi(k)}.$$

Дѣлая здѣсь $a = g$, находимъ

$$(2) \ldots\ldots \operatorname{Ind}_{g'} g \operatorname{Ind}_g g' \equiv 1 \pmod{\varphi(k)}.$$

Изъ (1) и (2) выводимъ

$$(3) \ldots\ldots \operatorname{Ind}_{g'} a \equiv \operatorname{Ind}_g a \operatorname{Ind}_{g'} g \pmod{\varphi(k)}.$$

Сравненія (2) и (3) рѣшаютъ вопросъ о переходѣ отъ основанія g къ основанію g'. На самомъ дѣлѣ, имѣя таблицу съ индексами по основанію g, мы можемъ изъ (2) опредѣлить значеніе $\operatorname{Ind}_{g'} g$, затѣмъ, умножая на $\operatorname{Ind}_{g'} g$ всѣ индексы въ таблицѣ, будемъ получать индексы по новому основанію g'.

Такъ какъ число всѣхъ первообразныхъ корней есть $\varphi(\varphi(k))$, то, приравнивая послѣдовательно значеніе g' всевозможнымъ первообразнымъ корнямъ, на основаніи (2) заключаемъ, что значеніе $\operatorname{Ind}_{g'} g$ перейдетъ тогда чрезъ всѣ $\varphi(\varphi(k))$ чиселъ $< \varphi(k)$ и простыхъ съ $\varphi(k)$. Соотвѣтственно этому наименьшій положительный вычетъ произведенія

$$\operatorname{Ind}_g a \operatorname{Ind}_{g'} g,$$

взятый по модулю $\varphi(k)$, мѣняя свое значеніе, достигнетъ минимума d, равнаго общему наибольшему дѣлителю чиселъ $\varphi(k)$ и $\operatorname{Ind}_g a$. Это есть минимумъ значенія $\operatorname{Ind}_{g'} a$ при всевозможныхъ основаніяхъ g'.

Для опредѣленія корня g', относительно котораго $\mathrm{Ind}_{g'} a$ достигаетъ означеннаго минимума, слѣдуетъ подобрать число t такъ, чтобы сумма

$$\frac{\mathrm{Ind}_g a}{d} + \frac{\varphi(k)}{d} t = h$$

представила число h простое относительно $\varphi(k)$. Это возможно вслѣдствіе того, что числа

$$\frac{\mathrm{Ind}_g a}{d} \quad \text{и} \quad \frac{\varphi(k)}{d}$$

взаимно простыя. Тогда искомый корень выразится такъ:

$$g' \equiv g^h \ (\mathrm{mod.}\ \varphi(k)).$$

ГЛАВА IX.

О функціональныхъ сравненіяхъ и о неприводимыхъ функціяхъ.

§ I. О функціяхъ, сравнимыхъ по двойному модулю. Рѣшеніе функціональнаго сравненія первой степени.

105. Способы изслѣдованія, примѣняемые нами въ предшествующихъ главахъ, могутъ быть перенесены и на функціи; многіе результаты, такимъ образомъ добытые, представляютъ большой интересъ.

Изображая чрезъ p какое нибудь простое число, а чрезъ $F(x)$ какую нибудь функцію неприводимую по модулю p, мы согласимся называть функціи $f(x)$ и $f_1(x)$ *сравнимыми по двойному модулю* $[p, F(x)]$, если разность $f(x) - f_1(x)$, по модулю p, дѣлится на $F(x)$ безъ остатка, то есть если имѣетъ мѣсто такое тожество:

$$f(x) - f_1(x) = F(x)\,\varphi(x) + p\psi(x),$$

гдѣ $\varphi(x)$ и $\psi(x)$ изображаютъ цѣлыя функціи (n^0 70). Символически это свойство выражаютъ такъ:

$$f(x) \equiv f_1(x), \ \text{mod.}\ [p, F(x)],$$

и говорятъ, что это есть *функціональное сравненіе*. Функція $f_1(x)$ называется вычетомъ функціи $f(x)$, и наоборотъ.

Надъ функціональными сравненіями позволяется производить такія же операціи какъ и надъ обыкновенными сравненіями: ихъ можно складывать, вычитать, умножать, а также и дѣлить съ соблюденіемъ условія, чтобы сокращаемый множитель не дѣлился по модулю p на модулярную функцію $F(x)$.

Обозначимъ степень $F(x)$ чрезъ n.

Раздѣливъ по модулю p функцію $f(x)$ на $F(x)$, получимъ въ остаткѣ нѣкоторую функцію $r(x)$ степени ниже n; это будетъ наименьшій вычетъ функціи $f(x)$ по модулю $[p, F(x)]$. Коеффиціенты въ выраженіи наименьшаго вычета можно увеличивать или уменьшать на произвольную кратность модуля p; вслѣдствіе этого можно предполагать, что они положительны и $< p$.

Если двѣ функціи $f(x)$ и $f_1(x)$ сравнимы по двойному модулю $[p, F(x)]$, то наименьшіе ихъ вычеты $r(x)$ и $r_1(x)$ сравнимы просто по модулю p, и наоборотъ.

Функціи, сравнимыя по модулю $[p, F(x)]$ съ одною какою нибудь функціей, сравнимы также и между собой, каждая съ каждой, по тому же модулю. Всѣ онѣ образуютъ одинъ классъ.

Число функцій въ каждомъ классѣ безконечно, но число различныхъ классовъ конечно; оно равно числу функцій степени ниже n, несравнимыхъ между собой по модулю p. Такія функціи получаются изъ общей формулы

$$a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n,$$

если давать коеффиціентамъ значенія

$$0, 1, 2, \ldots p-1.$$

Слѣдовательно ихъ число есть p^n.

106. Пусть

$$(1) \ldots\ldots\ldots\ldots r_1(x), r_2(x), \ldots r_{p^n-1}(x)$$

изображаютъ всѣ функціи степени ниже n, несравнимыя между собой по модулю p и отличныя отъ нуля.

Возьмемъ во вниманіе какую нибудь функцію $f(x)$, не дѣлящуюся по модулю p на $F(x)$, и обозначимъ соотвѣтственно чрезъ

(2). . . . . $s_1(x), s_2(x), \ldots s_{p^n-1}(x)$

наименьшіе вычеты произведеній

$$f(x)\, r_1(x),\ f(x)\, r_2(x), \ldots f(x)\, r_{p^n-1}(x),$$

по модулю $[p, F(x)]$.

Рядъ (2) будетъ только порядкомъ членовъ отличаться отъ (1); слѣдовательно имѣемъ

$$f(x)^{p^n-1}\, r_1(x)\, r_2(x) \ldots r_{p^n-1}(x) \equiv r_1(x)\, r_2(x) \ldots r_{p^n-1}(x),$$
$$\text{mod. } (p, F(x)).$$

Отсюда, сокращая обѣ части, получаемъ

(3) . . . . $f(x)^{p^n-1} \equiv 1 \quad \text{mod. } (p, F(x)).$

Это сравненіе для функцій представляетъ то же что теорема Фермата для чиселъ. Отсюда получаемъ, какъ слѣдствіе, сравненіе

(4). . . . . $f(x)^{p^n} \equiv f(x) \quad \text{mod. } (p, F(x)),$

которое справедливо для всякой функціи $f(x)$, какъ дѣлящейся на $F(x)$, такъ и не дѣлящейся.

Переходъ къ частному случаю $f(x) = x$ приводитъ къ слѣдующей теоремѣ.

Теорема. *Всякая функція $F(x)$, неприводимая по модулю p, есть дѣлитель функціи*

$$x^{p^n} - x.$$

по тому же модулю p.

Хотя теорема эта и составляетъ какъ будто частный случай сравненія (4), но въ свою очередь сравненіе (4) можетъ быть выведено какъ слѣдствіе послѣдней теоремы.

Это легче всего показать при помощи тожественнаго сравненія (n^0 74)

$$f(x)^{p^n} \equiv f(x^{p^n}) \pmod{p}.$$

На основаніи предыдущей теоремы имѣемъ

$$x^{p^n} \equiv x \mod. (p, F(x));$$

вслѣдствіе этого означенное сравненіе приводитъ къ такому:

$$f(x)^{p^n} \equiv f(x) \mod. [p, F(x)].$$

107. Функціональныя сравненія могутъ содержать функціи неизвѣстныя.

Сравненіе

$$(1)\ AX^m + A_1 X^{m-1} + \ldots + A_{m-1} X + A_m \equiv 0, \mod. [p, F(x)],$$

гдѣ A, A_1, ... A_m какія нибудь данныя функціи, а X функція искомая, называется функціональнымъ сравненіемъ m-ой степени; при этомъ предполагается, что коеффиціентъ A не дѣлится по модулю p на $F(x)$.

Коеффиціенты A, A_1, ... A_m могутъ быть замѣнены ихъ наименьшими вычетами.

Если $X = f(x)$ удовлетворяетъ (1), то ему удовлетворяетъ также всякая другая функція сравнимая съ $f(x)$ по модулю $[p, F(x)]$. Всѣ такія рѣшенія выражаются общею формулой

$$X \equiv f(x), \mod. [p, F(x)],$$

и не считаются за различныя.

Функціональное сравненіе первой степени

$$(2) \ldots\ldots\ldots\ AX \equiv 1, \mod. [p, F(x)],$$

въ которомъ извѣстный членъ равенъ 1, рѣшается просто посредствомъ ряда послѣдовательныхъ дѣленій по модулю p, какъ и численное сравненіе вида

$$ax \equiv 1 \pmod{p}.$$

Но можно рѣшеніе выразить явнымъ образомъ. На самомъ дѣлѣ, такъ какъ по предположенію коеффиціентъ A не дѣлится по модулю p на $F(x)$, то имѣетъ мѣсто сравненіе

$$A^{p^n} \equiv 1, \quad \text{mod.}\ [p, F(x)].$$

Оно можетъ быть написано такъ:

$$AA^{p^n-1} \equiv 1, \quad \text{mod.}\ [p, F(x)].$$

Отсюда видно, что

$$X \equiv A^{p^n-1}, \quad \text{mod.}\ [p, F(x)]$$

удовлетворяетъ сравненію (2).

Сравненіе m-ой степени можно всегда представить такъ, что коеффиціентъ у X^m будетъ равнымъ 1. Ибо, умножая обѣ части (1) на функцію B, удовлетворяющую условію

$$AB \equiv 1, \quad \text{mod.}\ [p, F(x)],$$

мы получаемъ сравненіе вида

$$X^m + B_1 X^{m-1} + \ldots + B_m \equiv 0, \quad \text{mod.}\ [p, F(x)],$$

равносильное (1), причемъ $B_1, B_2, \ldots B_m$ изображаютъ соотвѣтственно наименьшіе вычеты произведеній $A_1 B, A_2 B, \ldots A_m B$, взятые по модулю $[p, F(x)]$.

Такимъ образомъ сравненіе первой степени

(3). . . . . $AX \equiv A_1, \quad \text{mod.}\ [p, F(x)]$

во всякомъ частномъ случаѣ можетъ быть приведено къ виду

(4) . . . . $X \equiv B, \quad \text{mod.}\ [p, F(x)],$

что прямо даетъ рѣшеніе. Кромѣ (4), другихъ рѣшеній сравне-

ніе (3) имѣть не можетъ; ибо изображая чрезъ X_1 и X_2 двѣ какія нибудь функціи удовлетворяющія (3), имѣемъ

$$\left.\begin{aligned} AX_1 \equiv A_1 \\ AX_2 \equiv A_1 \end{aligned}\right\}, \quad \text{mod. } [p, F(x)],$$

откуда выводимъ

$$A(X_2 - X_1) \equiv 0, \quad \text{mod. } [p, F(x)].$$

А такъ какъ A по предположенію не дѣлится на $F(x)$, то слѣдовательно

$$X_2 \equiv X_1, \quad \text{mod. } [p, F(x)].$$

Это показываетъ, что функціи X_2 и X_1 составляютъ одно рѣшеніе.

§ II. Теорема Лагранжа. Слѣдствія.

108. **Теорема.** *Число рѣшеній функціональнаго сравненія не можетъ превышать его степени.*

Дѣйствительно, если X_1 удовлетворяетъ сравненію

$$(1)\ldots X^m + A_1 X^{m-1} + \ldots + A_m \equiv 0, \quad \text{mod. } [p, F(x)],$$

то раздѣляя полиномъ составляющій первую часть (1) на $X - X_1$, получаемъ въ остаткѣ функцію перемѣннаго x, дѣлящуюся на $[p, F(x)]$. Поэтому сравненіе (1) можно замѣнить слѣдующимъ:

$$(2)\ldots (X - X_1)(X^{m-1} + B_1 X^{m-2} + \ldots + B_{m-1}) \equiv 0,$$
$$\text{mod. } [p, F(x)].$$

Отсюда видно, что всякое рѣшеніе сравненія (1), отличное отъ X_1, должно удовлетворять сравненію

$$X^{m-1} + B_1 X^{m-2} + \ldots + B_{m-1} \equiv 0, \quad \text{mod. } [p, F(x)],$$

и если разъ доказано, что всякое сравненіе $(m-1)$-ой степени не можетъ имѣть болѣе $m-1$ рѣшеній, то тѣмъ самымъ дока-

зано, что и всякое сравненіе m-ой степени не можетъ имѣть болѣе m рѣшеній. Но сравненіе первой степени имѣетъ одно только рѣшеніе; поэтому сравненіе второй степени не можетъ имѣть болѣе двухъ рѣшеній; отсюда въ свою очередь слѣдуетъ, что сравненіе третьей степени не можетъ имѣть болѣе трехъ рѣшеній и такъ далѣе.

Слѣдствіе. *Если функціональное сравненіе, по виду m-ой степени,*

$$AX^m + A_1 X^{m-1} + A_2 X^{m-2} + \ldots + A_m \equiv 0, \ \text{mod.} [p, F(x)]$$

имѣетъ болѣе чѣмъ m рѣшеній, то всѣ коеффиціенты A, A_1, $A_2, \ldots A_m$ дѣлятся безъ остатка на $[p, F(x)]$, то есть

$$A \equiv A_1 \equiv A_2 \equiv \ldots \equiv A_m \equiv 0, \ \text{mod.} [p, F(x)].$$

109. Сравненіе

$$X^{p^n-1} \equiv 1, \ \text{mod.} [p, F(x)]$$

удовлетворяется всевозможными функціями, за исключеніемъ тѣхъ, которыя дѣлятся по модулю p на $F(x)$. Обозначивъ чрезъ $X_1, X_2, \ldots X_{p^n-1}$ функціи отличныя отъ нуля, получаемыя изъ общей формулы

$$a + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1},$$

гдѣ $a, a_1, \ldots a_n$ принимаютъ послѣдовательно значенія

$$0, 1, 2, \ldots p-1,$$

напишемъ сравненіе

$$(1)\ X^{p^n} - 1 - (X - X_1)(X - X_2) \ldots (X - X_{p^n-1}) \equiv 0, \quad \text{mod.} [p, F(x)].$$

Ему очевидно удовлетворяютъ функціи

$$X_1, X_2, \ldots X_{p^n-1},$$

между тѣмъ его степень ниже $p^n - 1$; поэтому коэффиціенты у различныхъ степеней X въ первой части (1) дѣлятся по модулю p на $F(x)$, и сравненіе представляетъ тожество.

Дѣлая въ (1) $X = 0$, получаемъ

$$X_1 X_2 X_3 \ldots X_{p^n-1} \equiv -1, \quad \text{mod.}\,[p, F(x)].$$

Это есть теорема Вильсона для функціональныхъ сравненій.

110. Обозначая, какъ и прежде, чрезъ n степень $F(x)$, мы замѣчаемъ, что всякое функціональное сравненіе

$$(1) \ldots\ldots\ldots f(X) \equiv 0, \quad \text{mod.}\,[p, F(x)],$$

степень котораго равна или выше p^n, можетъ быть замѣнено другимъ, степени ниже p^n. Для этого стоитъ только раздѣлить $f(X)$ на $X^{p^n} - X$, принявъ X за перемѣнное. Обозначая остатокъ полученный отъ этого дѣленія чрезъ $\psi(X)$, а частное чрезъ $\varphi(X)$, имѣемъ равенство

$$f(X) = (X^{p^n} - X)\,\varphi(X) + \psi(X),$$

прямо показывающее, что всякое рѣшеніе сравненія (1) удовлетворяетъ также и сравненію

$$(2) \ldots\ldots\ldots \psi(X) \equiv 0, \quad \text{mod.}\,[p, F(x)],$$

равно и наоборотъ. Слѣдовательно сравненіе (2) вполнѣ замѣняетъ (1); между тѣмъ степень (2) ниже степени (1).

Предположивъ теперь, что степень функціональнаго сравненія ниже p^n, не трудно доказать слѣдующую теорему.

Теорема. *Чтобъ функціональное сравненіе*

$$f(X) \equiv 0, \quad \text{mod.}\,[p, F(x)]$$

имѣло столько рѣшеній, сколько единицъ содержится въ его степени, необходимо и достаточно, чтобы всѣ коеффиціенты у различныхъ степеней X въ выраженіи остатка отъ дѣленія $X^{p^n} - X$ на $f(X)$ дѣлились по модулю p на $F(x)$.

На самомъ дѣлѣ, обозначивъ чрезъ $\varphi(X)$ и $\psi(X)$ частное и остатокъ отъ дѣленія $X^{p^n} - X$ на $f(X)$, имѣемъ равенство

$$(3) \ldots\ldots\ X^{p^n} - X = f(X)\,\varphi(X) + \psi(X),$$

которое показываетъ, что всѣ рѣшенія сравненія

$$(4) \ldots\ldots\ f(X) \equiv 0, \quad \text{mod.}\,[p, F(x)]$$

удовлетворяютъ также и сравненію

$$(5) \ldots\ldots\ \psi(X) \equiv 0, \quad \text{mod.}\,[p, F(x)].$$

А такъ какъ степень функціи $\psi(X)$ ниже степени $f(X)$, то, предположивъ, что (4) имѣетъ столько рѣшеній сколько единицъ содержится въ его степени, приходится заключить, что всѣ коеффиціенты въ выраженіи $\psi(x)$ дѣлятся на $[p, F(x)]$.

Остается доказать обратное: если всѣ коеффиціенты въ выраженіи $\psi(X)$ дѣлятся на $[p, F(x)]$, то сравненіе (4) имѣетъ тогда столько рѣшеній, сколько единицъ содержится въ его степени.

Для этого мы принимаемъ во вниманіе равенство (3) и замѣчаемъ, что сравненію

$$(6) \ldots\ f(X)\,\varphi(X) + \psi(X) \equiv 0, \quad \text{mod.}\,[p, F(x)]$$

удовлетворяетъ всякая функція X, вслѣдствіе чего число его рѣшеній равно p^n. Но, по предположенію, всѣ коеффиціенты въ выраженіи $\psi(X)$ сравнимы съ нулемъ по модулю $[p, F(x)]$; поэтому сравненіе (6) можно написать проще такъ:

$$(7) \ldots\ldots\ f(X)\,\varphi(X) \equiv 0, \quad \text{mod.}\,[p, F(x)].$$

Отсюда видно, что если произвольно взятая функція X не удовлетворяетъ сравненію (4), то тогда она навѣрно удовлетворяетъ сравненію

$$(8) \ldots\ldots\ \varphi(X) \equiv 0, \quad \text{mod.}\,[p, F(x)].$$

Слѣдовательно, еслибъ сравненіе (4) имѣло меньше рѣшеній чѣмъ единицъ содержится въ его степени, то (8) имѣло бы больше рѣшеній чѣмъ единицъ въ его степени, вслѣдствіе чего всѣ коеффиціенты въ выраженіи $\varphi(X)$ должны бы дѣлиться по модулю p на $F(x)$. Но это не имѣетъ мѣста; ибо коеффиціентъ у наивысшей степени перемѣннаго X въ выраженіи $\varphi(X)$ равенъ единицѣ.

Слѣдствіе. *Сравненіе*

$$X^m \equiv 1, \quad \text{mod.}\ [p, F(x)]$$

тогда только имѣетъ ровно m рѣшеній, когда m есть дѣлитель разности $p^n - 1$.

111. Изъ сравненія

$$(1) \ldots\ldots\ldots\ldots \quad x^{p^n} \equiv x, \quad \text{mod.}\ [p, F(x)],$$

какъ слѣдствіе, вытекаетъ

$$(2) \ldots\ldots\ldots\ldots \quad x^{p^{qn}} \equiv x, \quad \text{mod.}\ [p, F(x)].$$

Дѣйствительно, возвышая обѣ части (1) послѣдовательно въ степени $p^n, p^{2n}, p^{3n}, \ldots p^{(q-1)n}$, получаемъ рядъ сравненій

$$\left.\begin{array}{l} x^{p^n} \equiv x, \\ x^{p^{2n}} \equiv x^{p^n}, \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ x^{p^{qn}} \equiv x^{p^{(q-1)n}} \end{array}\right\} \text{mod.}\ [p, F(x)],$$

откуда прямо вытекаетъ (2).

Итакъ, если m есть кратное n, то имѣетъ мѣсто сравненіе

$$(3) \ldots\ldots\ldots\ldots \quad x^{p^m} \equiv x, \quad \text{mod.}\ [p, F(x)].$$

Но чтобы узнать всѣ случаи, когда (3) имѣетъ мѣсто, необходимо доказать слѣдующую лемму.

Лемма. *Если r не равно нулю и $< n$, то функція $x^{p^r} - x$ не дѣлится по модулю p на $F(x)$.*

На самомъ дѣлѣ, допустивъ противное, мы будемъ имѣть сравненіе

$$(4) \ldots\ldots\ldots\ldots x^{p^r} \equiv x, \quad \text{mod.}\, [p, F(x)],$$

откуда непосредственно вытекаетъ такое:

$$f(x^{p^r}) \equiv f(x), \quad \text{mod.}\, [p, F(x)],$$

причемъ $f(x)$ означаетъ произвольную функцію.

Но, съ другой стороны, мы имѣемъ сравненіе

$$f(x^{p^r}) \equiv f(x)^{p^r}, \quad (\text{mod.}\, p);$$

слѣдовательно

$$f(x)^{p^r} \equiv f(x), \quad \text{mod.}\, [p, F(x)].$$

Это приводитъ къ заключенію, что сравненію

$$(5) \ldots\ldots\ldots\ldots X^{p^r} \equiv X, \quad \text{mod.}\, [p, F(x)]$$

удовлетворяетъ всякая функція X; другими словами, оно имѣетъ p^n рѣшеній. Но это противорѣчитъ теоремѣ Лагранжа, ибо степень сравненія (5) ниже p^n; поэтому сравненіе (4) невозможно. Что и требовалось доказать.

Теперь легко доказать справедливость слѣдующей теоремы.

Теорема. *Сравненіе*

$$x^{p^m} \equiv x, \quad \text{mod.}\, [p, F(x)]$$

тогда только имѣетъ мѣсто, когда число m дѣлится на степень функціи $F(x)$.

Дѣйствительно, обозначая чрезъ n степень модулярной функціи, а чрезъ r остатокъ отъ дѣленія m на n, и полагая

$$m = nq + r,$$

мы замѣчаемъ, что сравненіе

$$(6) \dots\dots\dots\dots x^{p^m} \equiv x, \quad \text{mod. } [p, F(x)]$$

можно написать такъ:

$$(x^{p^{nq}})^{p^r} \equiv x, \quad \text{mod. } [p, F(x)],$$

а это, на основаніи вышедоказаннаго, приводится къ слѣдующему виду:

$$(7) \dots\dots\dots\dots x^{p^r} \equiv x, \quad \text{mod. } [p, F(x)].$$

Обратно, изъ (7) вытекаетъ (6), такъ что эти сравненія вполнѣ замѣняютъ одно другое. Но такъ какъ $r < n$, то изъ предшествующей леммы слѣдуетъ, что сравненіе (7) имѣетъ мѣсто только при $r = 0$. Слѣдовательно сравненіе (6) имѣетъ мѣсто только тогда, когда m дѣлится на n, что и требовалось доказать.

§ III. Разложеніе функціи $x^{p^n} - x$ на множители неприводимые по модулю p. Слѣдствія отсюда вытекающія.

112. **Теорема.** *Каковъ бы ни былъ простой модуль p, функція $x^{p^n} - x$ сравнима съ произведеніемъ всѣхъ неприводимыхъ функцій, степени которыхъ суть дѣлители числа n.*

На самомъ дѣлѣ, называя

$$f(x) = x^{p^n} - x,$$

имѣемъ

$$f'(x) \equiv -1, \quad (\text{mod. } p),$$

откуда видно, что $f(x)$ и $f'(x)$ относительно простыя по модулю p; слѣдовательно въ разложеніи функціи $x^{p^n} - x$ на неприводимые множители нѣтъ кратныхъ множителей (n^0 75).

Изображая чрезъ $F(x)$ какую угодно неприводимую функцію, степень которой дѣлитъ n, имѣемъ

$$x^{p^n} - x \equiv 0, \quad \text{mod. } [p, F(x)].$$

Это показываетъ, что $F(x)$ входитъ въ составъ функціи $x^{p^n}-x$.

Обратно, степень всякой неприводимой функціи, входящей въ составъ $x^{p^n}-x$, есть дѣлитель числа n. Ибо, обозначивъ чрезъ $F(x)$ какой нибудь изъ неприводимыхъ дѣлителей функціи $x^{p^n}-x$, имѣемъ сравненіе

$$x^{p^n}-x\equiv 0,\ \ \text{mod.}\ [p, F(x)],$$

на основаніи котораго заключаемъ, что n дѣлится на степень $F(x)$ (n^0 111).

Итакъ, въ составъ функціи $x^{p^n}-x$ входятъ всѣ неприводимыя функціи, степень которыхъ дѣлитъ n; кромѣ этихъ никакія другія функціи въ составъ $x^{p^n}-x$ не входятъ; слѣдовательно функція $x^{p^n}-x$ сравнима съ произведеніемъ всѣхъ означенныхъ неприводимыхъ функцій. Что и слѣдовало доказать.

113. Изъ послѣдней теоремы вытекаетъ простой способъ составленія произведенія всѣхъ неприводимыхъ функцій данной степени.

Дѣйствительно, обозначимъ чрезъ Φ_n произведеніе неприводимыхъ функцій n-ой степени, и допустимъ, что намъ извѣстны всѣ функціи Φ_1, Φ_2, . . . до Φ_{n-1} включительно. Обозначивъ чрезъ

$$1,\ n_1,\ n_2, \ldots n_i,\ n$$

всѣ дѣлители числа n, имѣемъ сравненіе

$$x^{p^n}-x\equiv \Phi_1\,\Phi_{n_1}\,\Phi_{n_2}\ldots\Phi_{n_i}\,\Phi_n\quad (\text{mod.}\,p),$$

во второй части котораго функціи Φ_1, Φ_2, . . . Φ_{n_i} извѣстны. Слѣдовательно функція $x^{p^n}-x$ дѣлится по модулю p безъ остатка на произведеніе $\Phi_1\,\Phi_2\ldots\Phi_{n_i}$ и частное равно искомой функціи Φ_n.

Замѣчая теперь, что

$$\Phi_1=x(x-1)\,(x-2)\ldots(x-p+1)\equiv x^p-x,\ (\text{mod.}\,p),$$

мы получаемъ для Φ_2 такую формулу

$$\Phi_2 \equiv \frac{x^{p^2} - x}{x^p - x} \pmod{p}.$$

Слѣдующія функціи можно выразить такъ:

$$\Phi_3 \equiv \frac{x^{p^3} - x}{x^p - x} \pmod{p},$$

$$\Phi_4 \equiv \frac{x^{p^4} - x}{x^{p^2} - x} \pmod{p},$$

$$\Phi_5 \equiv \frac{x^{p^5} - x}{x^p - x} \pmod{p},$$

$$\Phi_6 \equiv \frac{(x^{p^6} - x)(x^p - x)}{(x^{p^3} - x)(x^{p^2} - x)} \pmod{p},$$

и такъ далѣе. Для простаго n имѣемъ

$$\Phi_n \equiv \frac{x^{p^n} - x}{x^p - x} \pmod{p}.$$

Отсюда непосредственно заключаемъ, что число неприводимыхъ функцій n-ой степени, при простомъ n, равно

$$\frac{p^n - p}{n}.$$

114. Чтобы составить выраженіе функціи Φ_n для какого угодно n, мы предложимъ себѣ найти такую функцію $f(n)$ цѣлаго перемѣннаго n, которая удовлетворяла бы условію

$$(1) \quad \ldots\ldots f(1)\, f(n_1)\, f(n_2) \ldots f(n_i)\, f(n) = x^{p^n} - x,$$

причемъ $1, n_1, n_2, \ldots n_i, n$ изображаютъ всѣ дѣлители числа n. Намъ уже извѣстно, какъ рѣшается подобный вопросъ (n^0 14);

для этого мы разлагаемъ число n на произведеніе простыхъ множителей

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_m^{\alpha_m}$$

и составляемъ рядъ частныхъ

$$a_1 = \frac{n}{q_1},\quad a_1' = \frac{n}{q_2},\quad a_1'' = \frac{n}{q_3}, \ldots,$$

$$a_2 = \frac{n}{q_1 q_2},\quad a_2' = \frac{n}{q_1 q_3},\quad a_2'' = \frac{n}{q_2 q_3}, \ldots,$$

$$a_3 = \frac{n}{q_1 q_2 q_3},\quad a_3' = \frac{n}{q_1 q_2 q_4}, \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$a_m = \frac{n}{q_1 q_2 \ldots q_m}.$$

Число чиселъ a_i, a_i', a_i'', ... равно очевидно числу сочетаній изъ m элементовъ по i.

Полагая теперь для сокращенія

$$\Pi(x^{p^{a_1}} - x) = (x^{p^{a_1}} - x)(x^{p^{a_1'}} - x)(x^{p^{a_1''}} - x)\ldots,$$

$$\Pi(x^{p^{a_2}} - x) = (x^{p^{a_2}} - x)(x^{p^{a_2'}} - x)(x^{p^{a_2'''}} - x)\ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\Pi(x^{p^{a_m}} - x) = x^{p^{a_m}} - x,$$

мы имѣемъ слѣдующую формулу для искомой функціу $f(n)$:

$$\textbf{(2)}\quad f(n) = \frac{(x^{p^n} - x)\,\Pi(x^{p^{a_2}} - x)\,\Pi(x^{p^{a_4}} - x)\,\Pi(x^{p^{a_6}} - x)\ldots}{\Pi(x^{p^{a_1}} - x)\,\Pi(x^{p^{a_3}} - x)\,\Pi(x^{p^{a_5}} - x)\ldots}.$$

Для $n = 1$, на основаніи (1) заключаемъ прямо

$$f(1) = x^p - x;$$

это совпадаетъ съ выраженіемъ функціи Φ_1, даннымъ въ предшествующемъ номерѣ; слѣдовательно

$$(3) \ldots\ldots\ldots\ldots\ldots \Phi_1 = f(1).$$

Для $n = 2$ имѣемъ

$$f(1)\, f(2) = x^{p^2} - x,$$

и сверхъ того

$$\Phi_1\, \Phi_2 \equiv x^{p^2} - x \pmod{p};$$

откуда заключаемъ

$$\Phi_1\, \Phi_2 \equiv f(1)\, f(2) \pmod{p}.$$

Замѣчая, что $\Phi_1 = f(1)$ и сокращая обѣ части послѣдняго сравненія на Φ_1, получаемъ

$$\Phi_2 \equiv f(2) \pmod{p}.$$

Для $n = 3$ имѣемъ

$$\Phi_1\, \Phi_3 \equiv x^{p^3} - x \pmod{p}$$

$$f(1)\, f(3) = x^{p^3} - x;$$

отсюда выводимъ

$$\Phi_1\, \Phi_3 \equiv f(1)\, f(3) \pmod{p},$$

и, сокращая обѣ части на $\Phi_1 = f(1)$, получаемъ

$$\Phi_3 \equiv f(3) \pmod{p}.$$

Продолжая полагать далѣе $n = 4, 5, \ldots$ мы убѣждаемся такимъ образомъ, что для всякаго n имѣетъ мѣсто формула

$$(4) \ldots \Phi_n \equiv \frac{(x^{p^n} - x)\, \Pi(x^{p^{a_2}} - x)\, \Pi(x^{p^{a_4}} - x) \ldots}{\Pi(x^{p^{a_1}} - x)\, \Pi(x^{p^{a_3}} - x) \ldots} \pmod{p}.$$

Если обозначимъ чрезъ $\lambda_1, \lambda_1', \ldots$ тѣ члены въ произведеніи $q_1^{\alpha_1-1} q_2^{\alpha_2-1} \ldots q_m^{\alpha_m-1} (q_1-1)(q_2-1)\ldots(q_m-1)$, которымъ предшествуетъ знакъ $+$, а чрезъ $\lambda_2, \lambda_2', \ldots$ тѣ, которымъ предшествуетъ знакъ $-$, то можемъ написать

$$(5) \ldots\ldots\ldots\ldots \varphi(n) = \Sigma\lambda_1 - \Sigma\lambda_2,$$

и сообразно съ этимъ формула (4) можетъ быть представлена такъ:

$$(6) \ldots\ldots\ldots\ldots \Phi_n \equiv \frac{\Pi(x^{p^{\lambda_1}} - x)}{\Pi(x^{p^{\lambda_2}} - x)} \pmod{p}.$$

115. Функція перемѣннаго x, составляющая вторую часть послѣдней формулы, представляетъ цѣлую функцію не только въ томъ смыслѣ, что дѣленіе слѣдуетъ производить по модулю p, какъ это здѣсь подразумѣвается, но даже и въ смыслѣ обыкновеннаго дѣленія, такъ что можно написать

$$\Phi_n = \frac{\Pi(x^{p^{\lambda_1}} - x)}{\Pi(x^{p^{\lambda_2}} - x)}.$$

Чтобъ удостовѣриться въ этомъ, достаточно принять въ соображеніе нижеслѣдующія двѣ леммы.

Лемма 1. *Если количество x удовлетворяетъ двумъ уравненіямъ*

$$x^{p^a} - x = 0, \quad x^{p^b} - x = 0, \quad (a \geqq b),$$

и если оно не удовлетворяетъ никакому уравненію вида

$$x^{p^c} - x = 0$$

при условіи $0 < c < b$, то тогда a дѣлится на b.

Дѣйствительно, изъ уравненія $x^{p^b} - x = 0$ какъ слѣдствіе вытекаетъ уравненіе

$$x^{p^{qb}} - x = 0,$$

при чемъ q изображаетъ произвольное положительное число.

Съ другой стороны, обозначивъ соотвѣтственно чрезъ q и r частное и остатокъ отъ дѣленія a на b, уравненіе $x^{p^a}-x=0$ можно написать такъ:

$$(x^{p^{qb}})^{p^r}-x=0,$$

что на основаніи предыдущаго приводится къ слѣдующему виду

$$x^{p^r}-x=0.$$

Но $r<b$; слѣдовательно $r=0$. Это показываетъ, что a дѣлится на b, что и слѣдовало доказать.

Слѣдствіе. *Если количество x удовлетворяетъ одновременно двумъ уравненіямъ*

$$x^{p^a}-x=0, \quad x^{p^{a'}}-x=0,$$

то оно удовлетворяетъ и третьему уравненію

$$x^{p^d}-x=0,$$

гдѣ d есть общій наибольшій дѣлитель чиселъ a и a'.

Лемма 2. *Каковы бы ни были два числа n и $n'<n$, если разложимъ n на простые множители*

$$n=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_m^{\alpha_m}$$

и затѣмъ составимъ произведеніе

$$\varphi(n)=n\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_m}\right)=\sum\lambda_1-\sum\lambda_2,$$

то, какъ въ полиномѣ $\Sigma\lambda_1$, такъ и въ полиномѣ $\Sigma\lambda_2$, число членовъ, дѣлящихся на n', одинаково.

Справедливость этой леммы провѣряется непосредственно.

116. Переходя теперь къ функціи

$$(1) \ldots\ldots\ldots\ldots\ldots \frac{\Pi(x^{p^{\lambda_1}}-x)}{\Pi(x^{p^{\lambda_2}}-x)},$$

мы обозначимъ чрезъ $x-\omega$ какой нибудь изъ линейныхъ множителей ея знаменателя, и пусть

$$(2) \; \ldots\ldots\ldots\ldots \; x^{p^a}-x=0$$

есть уравненіе, которому удовлетворяетъ значеніе $x=\omega$ при самомъ маломъ показателѣ a, такъ что ω не удовлетворяетъ никакому другому уравненію вида (2) съ показателемъ у p больше нуля и меньше a.

Предположивъ это, мы замѣчаемъ, что множитель $x-\omega$ входитъ въ составъ числителя

$$\Pi(x^{p^{\lambda_1}}-x)$$

съ показателемъ равнымъ числу членовъ полинома $\Sigma\lambda_1$, дѣлящихся на a, а въ составъ знаменателя

$$\Pi(x^{p^{\lambda_2}}-x),$$

— съ показателемъ равнымъ числу членовъ полинома $\Sigma\lambda_2$, дѣлящихся на a.

Но $a<n$, поэтому на основаніи вышеизложеннаго заключаемъ, что множитель $x-\omega$ входитъ съ одинаковымъ показателемъ какъ въ составъ числителя функціи (1), такъ и въ составъ ея знаменателя. Слѣдовательно функція (1) есть цѣлая.

117. Изъ выраженія функціи Φ_n видно, что ея степень равна разности

$$\Sigma p^{\lambda_1}-\Sigma p^{\lambda_2};$$

слѣдовательно число неприводимыхъ функцій n-ой степени, по модулю p есть

$$(1) \; \ldots\ldots\ldots\ldots \; \nu=\frac{\Sigma p^{\lambda_1}-\Sigma p^{\lambda_2}}{n}.$$

Въ частномъ случаѣ, когда n есть степень простаго числа q, имѣемъ

$$(2) \; \ldots\ldots\ldots\ldots \; \nu=\frac{p^n-p^{\frac{n}{q}}}{n}.$$

Изъ (1) легко вывести два предѣла для ν. Для этого мы замѣчаемъ равенство

$$\sum\lambda_1^i - \sum\lambda_2^i = n^i\left(1-\frac{1}{q_1^i}\right)\left(1-\frac{1}{q_2^i}\right)\ldots\left(1-\frac{1}{q^i_m}\right),$$

изъ котораго заключаемъ: во первыхъ,

$$(3) \ldots\ldots\ldots\ldots \Sigma\lambda_1^i - \Sigma\lambda_2^i < n^i;$$

во вторыхъ, если $i > 1$,

$$(4) \quad \sum\lambda_1^i - \sum\lambda_2^i \geqq n^i\left(1-\frac{1}{q_1^2}\right)\left(1-\frac{1}{q_2^2}\right)\ldots\left(1-\frac{1}{q^2_m}\right).$$

Съ другой стороны имѣемъ очевидное неравенство

$$\left(1-\frac{1}{q_1^2}\right)\left(1-\frac{1}{q_2^2}\right)\ldots\left(1-\frac{1}{q^2_m}\right) > \left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{4^2}\right)\ldots,$$

вторая часть котораго равна $\frac{1}{2}$; слѣдовательно изъ (4) выводимъ

$$(5) \ldots\ldots\ldots \Sigma\lambda_1^i - \Sigma\lambda_2^i > \tfrac{1}{2}n^i, \quad (i > 1).$$

Переходя теперь къ формулѣ (1), мы представляемъ вторую часть въ видѣ ряда

$$\nu = \frac{\log p}{n}\left[\Sigma\lambda_1 - \Sigma\lambda_2\right] + \frac{\log^2 p}{n.1.2}\left[\Sigma\lambda_1^2 - \Sigma\lambda_2^2\right] + \frac{\log^3 p}{n.1.2.3}\left[\Sigma\lambda_1^3 - \Sigma\lambda_2^3\right] + \ldots$$

Отсюда съ помощью (3) выводимъ

$$\nu < \frac{n\log p}{n} + \frac{(n\log p)^2}{n.1.2} + \frac{(n\log p)^3}{n.1.2.3} + \ldots,$$

или

$$(6) \ldots\ldots\ldots\ldots\ldots \nu < \frac{p^n - 1}{n}.$$

Чтобъ получить нисшій предѣлъ для числа ν, мы замѣчаемъ, что разность $\Sigma\lambda_1 - \Sigma\lambda_2$ положительна, вслѣдствіе чего изъ послѣдней формулы для ν вытекаетъ неравенство

$$\nu > \frac{\log^2 p}{n.1.2}\left[\Sigma\lambda_1^2 - \Sigma\lambda_2^2\right] + \frac{\log^3 p}{n.1.2.3}\left[\Sigma\lambda_1^3 - \Sigma\lambda_2^3\right] + \ldots$$

Отсюда съ помощью (5) выводимъ

$$\nu > \frac{(n \log p)^2}{2n.1.2} + \frac{(n \log p)^3}{2n.1.2.3} + \ldots,$$

или

(7) . . . . $\nu > \frac{p^n - 1}{2n} - \frac{\log p}{2}.$

Неравенство (7) показываетъ, что число ν никогда не равно нулю, и что оно удаляется до безконечности, если n безпредѣльно возрастаетъ.

118. Отыскиваніе неприводимыхъ функцій по данному модулю составляетъ задачу, которую мы не умѣемъ рѣшать иначе, какъ съ помощью послѣдовательныхъ испытаній. Рѣдко удается доказать прямо приводимость или неприводимость функціи извѣстнаго вида; потому нижеслѣдующая теорема заслуживаетъ особаго вниманія.

Теорема. *Если a не дѣлится на p, то функція*

$$x^p - x + a$$

неприводима по модулю p.

Дѣйствительно, допустимъ противное и положимъ

(1) . . . . $x^p - x + a \equiv f f_1 \pmod{p}$,

причемъ f изображаетъ неприводимую функцію степени ниже p.

Возвысивъ обѣ части (1) въ степень p находимъ

(2). . . . . $x^{p^2} - x^p + a \equiv f^p f_1^p \pmod{p}$.

Возвысивъ обѣ части послѣдняго сравненія еще въ степень p, находимъ

(3) . . . . $x^{p^3} - x^{p^2} + a \equiv f^{p^2} f_1^{p^2} \pmod{p}$.

Продолжая дѣйствовать подобнымъ образомъ далѣе, мы дойдемъ до сравненія

$$x^{p^m} - x^{p^{m-1}} + a \equiv f^{p^m} f_1^{p^m} \pmod{p},$$

гдѣ m равно степени функціи f.

Складывая почленно сравненія (1), (2), . . . до m-го включительно и произведя сокращенія, получаемъ такое функціональное сравненіе:

$$x^{p^m} - x + ma \equiv 0, \text{ mod. } [f, p].$$

А такъ какъ

$$x^{p^m} - x \equiv 0, \text{ mod. } [f, p],$$

то слѣдовательно

$$ma \equiv 0, \text{ mod. } [f, p],$$

или, проще,

$$ma \equiv 0 \pmod{p}.$$

Но это невозможно, ибо ни m ни a не дѣлятся на p; слѣдовательно сравненіе (1) невозможно, что и слѣдовало доказать.

§ IV. О показателяхъ, принадлежащихъ функціямъ по данному модулю.

119. Положивъ, что $f(x)$ не дѣлится по модулю p на неприводимую функцію $F(x)$, составимъ наименьшіе вычеты функцій

(1) . . . . $f(x), f(x)^2, f(x)^3, \ldots f(x)^m, \ldots$

по модулю $[p, F(x)]$ и изобразимъ ихъ соотвѣтственно чрезъ

(2) . . . . $r_1, r_2, r_3, \ldots r_m, \ldots$

Ни одна изъ функцій (2) не равна нулю; но есть между ними повторяющіяся. Пусть

$$r_i = r_k,$$

причемъ $i > k$; тогда будемъ имѣть

$$f(x)^i \equiv f(x)^k, \text{ mod. } [p, F(x)],$$

откуда выводимъ

$$f(x)^{i-k} \equiv 1, \text{ mod. } [p, F(x)].$$

Слѣдовательно въ ряду (2) есть функція, которая равна 1. Пусть

$$r_m = 1,$$

и положимъ, что значекъ m есть самый малый, при которомъ $r_m = 1$, такъ что ни одна изъ функцій $r_1, r_2, \ldots r_{m-1}$ не равна 1; число m, такимъ образомъ опредѣленное, есть *показатель, принадлежащій функціи $f(x)$ по модулю $[p, F(x)]$.*

Положивъ это, и затѣмъ разсуждая, какъ въ предыдущей главѣ, мы легко удостовѣряемся въ справедливости слѣдующихъ основныхъ теоремъ.

Теорема 1. *Если функція $f(x)$, по модулю $[p, F(x)]$, принадлежитъ къ показателю m, то наименьшіе вычеты функцій*

$$1, f(x), f(x)^2, \ldots f(x)^{m-1}, f(x)^m, \ldots$$

составляютъ періодическій рядъ; періодъ начинается съ перваго члена и содержитъ ровно m членовъ, между которыми нѣтъ равныхъ.

Слѣдствіе 1. *Если функція $f(x)$ по модулю $[p, F(x)]$ принадлежитъ къ показателю m, то, чтобы имѣло мѣсто функціональное сравненіе*

$$f(x)^i \equiv f(x)^{i'}, \text{ mod. } [p, F(x)],$$

необходимо и достаточно условіе

$$i \equiv i' \pmod{m}.$$

Слѣдствіе 2. *Какова бы ни была функція $f(x)$, показатель, принадлежащій къ ней по модулю $[p, F(x)]$, дѣлитъ разность $p^n - 1$, при чемъ n изображаетъ степень $F(x)$.*

Теорема 2. *Если функція $f(x)$ по модулю $[p, F(x)]$ принадлежитъ къ показателю m, то степень $f(x)^i$ по тому же модулю принадлежитъ къ показателю $\frac{m}{d}$, гдѣ d изображаетъ общій наибольшій дѣлитель m и i.*

Теорема 3. *Если двѣ функціи $f(x)$ и $f_1(x)$ по модулю $[p, F(x)]$ принадлежатъ соотвѣтственно къ показателямъ m и m_1, то можно найти такую функцію $\varphi(x)$, которая, по тому же модулю, будетъ принадлежать къ показателю равному наименьшему кратному чиселъ m и m_1.*

Теорема 4. *Каковъ бы ни былъ дѣлитель m числа p^n-1, всегда существуетъ ровно $\varphi(m)$ функцій, принадлежащихъ по модулю $[p, F(x)]$ къ показателю m.*

Слѣдовательно существуетъ ровно $\varphi(p^n-1)$ функцій, принадлежащихъ къ показателю p^n-1. Онѣ суть *первообразные* корни функціи $F(x)$.

Если G есть первообразный корень функціи $F(x)$, то всякая функція $f(x)$, не дѣлящаяся по модулю p на $F(x)$, можетъ быть представлена такъ:

$$f(x) \equiv G^m \text{ mod. } [p, F(x)],$$

причемъ

$$0 \leqq m < p^n - 1.$$

Число m опредѣляется такимъ образомъ вполнѣ; оно называется *индексомъ* функціи $f(x)$. Функція G служитъ *основаніемъ* системы индексовъ.

Главныя свойства индексовъ функцій таковы, какъ и свойства индексовъ чиселъ.

Чтобъ не повторяться, мы не станемъ входить въ дальнѣйшія подробности по этому предмету; перейдемъ къ изложенію другой теоріи, которая примѣняется исключительно къ функціональнымъ сравненіямъ и, по существу, близко подходитъ къ тому, что было нами здѣсь изложено.

§ V. О надпоказателяхъ, принадлежащихъ къ функціямъ по данному модулю.

120. Какова бы ни была функція $f(x)$, въ ряду

(1) . . . . $f(x)^p, f(x)^{p^2}, f(x)^{p^3}, \ldots$

всегда найдется такая степень, которая по модулю $[p, F(x)]$ будетъ сравнима съ $f(x)$. Это очевидно на основаніи теоремы Ферматa, по которой имѣемъ

$$f(x)^{p^n} \equiv f(x), \text{ mod. } [p, F(x)].$$

Въ случаѣ, если $f(x) \equiv 0$, mod. $[p, F(x)]$, на мѣсто $f(x)$ можно подставить нуль; тогда означенный рядъ будетъ состоять изъ однихъ нулей, что не можетъ представлять какого нибудь интереса. Поэтому-то мы постоянно будемъ здѣсь подразумѣвать, что $f(x)$ не дѣлится по модулю p на $F(x)$.

Согласившись обозначать чрезъ μ наименьшее число, неравное нулю, при которомъ имѣетъ мѣсто сравненіе

$$f(x)^{p^\mu} \equiv f(x), \text{ mod. } [p, F(x)],$$

мы будемъ называть μ *надпоказателемъ, принадлежащимъ функціи* $f(x)$ *по модулю* $[p, F(x)]$.

Въ связи съ этимъ намъ придется различать дѣлители формы

$$p^\mu - 1$$

на *первообразные* и *непервообразные*. Первообразными будемъ называть такіе, которые не дѣлятъ ни одного изъ чиселъ

$$p - 1, p^2 - 1, \ldots p^{\mu-1} - 1.$$

Можно сказать иначе такъ: дѣлитель d формы $p^\mu - 1$ есть первообразный или непервообразный, смотря по тому принадлежитъ ли число p по модулю d къ показателю μ или къ показателю $< \mu$.

Принимая въ соображеніе вышесказанное не трудно доказать слѣдующую теорему.

Теорема 1. *Если функція* $f(x)$ *по модулю* $[p, F(x)]$ *принадлежитъ къ показателю* m *и къ надпоказателю* μ, *то* m *есть первообразный дѣлитель формы* $p^\mu - 1$.

Дѣйствительно, мы имѣемъ сравненіе

$$(5) \dots\dots\dots f(x)^{p^\mu} \equiv f(x), \text{ mod. } [p, F(x)],$$

обѣ части котораго можно сократить на $f(x)$ и написать

$$f(x)^{p^\mu - 1} \equiv 1, \text{ mod. } [p, F(x)].$$

Отсюда слѣдуетъ, что разность $p^\mu - 1$ дѣлится на m, ибо $f(x)$ принадлежитъ къ показателю m.

Остается показать, что m есть первообразный дѣлитель разности $p^\mu - 1$. Для этого допустимъ противное, пусть m дѣлитъ $p^{\mu'} - 1$, при чемъ $\mu' < \mu$. На основаніи сравненія

$$p^{\mu'} - 1 \equiv 0 \pmod{m}$$

заключаемъ

$$f(x)^{p^{\mu'} - 1} \equiv 1, \text{ mod. } [p, F(x)],$$

откуда выводимъ

$$f(x)^{p^{\mu'}} \equiv f(x), \text{ mod. } [p, F(x)].$$

Но послѣднее сравненіе противорѣчитъ предположенію, что μ есть самое малое число, при которомъ имѣетъ мѣсто (5); слѣдовательно m есть первообразный дѣлитель формы $p^\mu - 1$, что и слѣдовало доказать.

Слѣдствіе. *Надпоказатель* μ, *къ которому принадлежитъ произвольно взятая функція* $f(x)$, *есть дѣлитель степени модулярной функціи.*

Ибо, по извѣстному свойству показателя m, имѣемъ

$$p^n - 1 \equiv 0 \pmod{m};$$

а такъ какъ p по модулю m принадлежитъ къ показателю μ, то n дѣлится на μ.

Теорема 2. *Если μ есть надпоказатель, къ которому принадлежитъ функція $f(x)$ по модулю $[p, F(x)]$, то рядъ наименьшихъ вычетовъ степеней*

$$f(x),\ f(x)^p,\ f(x)^{p^2}, \ldots f(x)^{p^{\mu-1}},\ f(x)^{p^\mu}, \ldots,$$

по тому же модулю, есть періодическій; періодъ начинается съ перваго члена и содержитъ ровно μ членовъ; всѣ члены въ періодѣ различны и ни одинъ не равенъ 1, если только функція $f(x)$ не сравнима съ единицей.

На самомъ дѣлѣ, такъ какъ, по предположенію, имѣемъ

$$f(x)^{p^\mu} \equiv f(x), \text{ mod. } [p, F(x)],$$

то

$$f(x)^{p^{i+\mu}} \equiv f(x)^{p^i}, \text{ mod. } [p, F(x)].$$

Отсюда видно, что вычеты функцій

(6) . . . . $f(x),\ f(x)^p, \ldots f(x)^{p^{\mu-1}}, \ldots$

образуютъ періодическій рядъ, что періодъ начинается съ перваго члена и содержимъ μ членовъ.

Чтобы доказать теперь, что въ періодѣ нѣтъ двухъ равныхъ членовъ, мы допустимъ противное:

$$f(x)^{p^i} \equiv f(x)^{p^{i'}}, \text{ mod. } [p, F(x)],$$

гдѣ $i < i' < \mu$. Возвышая обѣ части въ степень p, получаемъ

$$f(x)^{p^{i+1}} \equiv f(x)^{p^{i'+1}}, \text{ mod. } [p, F(x)].$$

Возвышая еще обѣ части въ степень p, получаемъ

$$f(x)^{p^{i+2}} \equiv f(x)^{p^{i'+2}}, \text{ mod. } [p, F(x)]$$

и т. д. Слѣдовательно

$$f(x)^{p^{\mu+i-i'}} \equiv f(x)^{p^\mu}, \text{ mod. } [p, F(x)],$$

или

$$f(x)^{p^{\mu-(i'-i)}} \equiv f(x), \text{ mod. } [p, F(x)],$$

что невозможно; ибо показатель $\mu-(i'-i)<\mu$. Слѣдовательно періодъ дѣйствительно состоитъ изъ различныхъ членовъ.

Остается еще показать, что ни одна изъ функцій (6) не сравнима съ 1.

Изъ сравненія

$$f(x)^{p^i}\equiv 1,\ \text{mod.}\ [p, F(x)]$$

вытекаетъ, что p^i дѣлится на m; слѣдовательно m есть степень p. Но, съ другой стороны, m есть дѣлитель p^n-1; поэтому слѣдуетъ положить $m=1$. Это приводитъ къ заключенію, что $f(x)=1$.

Итакъ, если $f(x)$ не равна 1, то ни одинъ членъ въ ряду (6) не сравнимъ съ 1.

Наша теорема такимъ образомъ доказана вполнѣ.

Слѣдствіе. *Если имѣетъ мѣсто функціональное сравненіе*

$$f(x)^{p^{\mu'}}\equiv f(x)^{p^{\mu''}},\ \text{mod.}\ [p, F(x)],$$

то имѣетъ мѣсто и числовое сравненіе

$$\mu'\equiv\mu''\ (\text{mod.}\ \mu),$$

и наоборотъ.

§ VI. Число функцій, принадлежащихъ къ данному надпоказателю.

121. Обозначая чрезъ n степень неприводимой (по модулю p) функціи $F(x)$, а чрезъ μ какой-нибудь дѣлитель числа n, мы покажемъ какъ опредѣляется число функцій, принадлежащихъ, по модулю $[p, F(x)]$, къ надпоказателю μ.

Легко замѣтить, что искомое число есть кратность μ. На самомъ дѣлѣ, допустивъ что X принадлежитъ къ надпоказателю μ, мы замѣчаемъ, что X удовлетворяетъ сравненію

$$X^{p^{\mu}}\equiv X,\ \text{mod.}\ [p, F(x)],$$

а тѣмъ самымъ и сравненію

(1) . . . . $X^{p^\mu - 1} \equiv 1$, mod. $[p, F(x)]$,

ибо X, по предположенію, не дѣлится на $F(x)$.

Съ другой стороны, такъ какъ μ дѣлитъ n, то $p^\mu - 1$ дѣлитъ $p^n - 1$, и слѣдовательно функція

$$X^{p^\mu - 1} - 1$$

дѣлитъ

$$X^{p^n - 1} - 1,$$

вслѣдствіе чего заключаемъ, что сравненіе (1) имѣетъ ровно $p^\mu - 1$ рѣшеній (n^0 110). Между ними слѣдуетъ искать всѣ функціи, принадлежащія къ надпоказателю μ.

Еслибъ между корнями сравненія (1) не было ни одного, принадлежащаго къ надпоказателю μ, тогда пришлось бы заключить о несуществованіи функцій, принадлежащихъ къ надпоказателю μ: ихъ число равнялось бы тогда нулю. Но если допустимъ существованіе одной функціи X, принадлежащей къ надпоказателю μ, то сейчасъ замѣчаемъ, что и всѣ функціи въ ряду

(2) . . . . $X, X^p, X^{p^2}, \ldots X^{p^{\mu-1}}$

принадлежатъ къ надпоказателю μ; онѣ различны и удовлетворяютъ сравненію (1).

Слѣдовательно, если искомое число не равно нулю, то оно или равно μ, или больше μ. Допустимъ, что оно больше μ, и пусть X_1 есть функція не содержащаяся въ (2), но принадлежащая къ надпоказателю μ. Тогда всѣ функціи въ ряду

(3) . . . . $X_1, X_1^p, X_1^{p^2}, \ldots X_1^{p^{\mu-1}}$

будутъ принадлежать къ надпоказателю μ. Онѣ различны не только между собою но и по отношенію къ (2); ибо изъ сравненія

$$X_1^{p^i} \equiv X^{p^{i'}}, \text{ mod. } [p, F(x)],$$

выводимъ

$$X_1^{p^n} \equiv X^{p^{n+i'-i}}, \text{ mod. } [p, F(x)],$$

или

$$X_1 \equiv X^{p^{n+i'-i}}, \text{ mod. } [p, F(x)],$$

откуда слѣдуетъ, что X_1 содержится въ (2), что противорѣчитъ предположенію.

Если теперь допустимъ, что кромѣ (2) и (3), существуетъ еще одна какая нибудь функція, принадлежащая къ надпоказателю μ, то подобно предыдущему мы обнаружимъ существованіе еще μ новыхъ функцій, принадлежащихъ къ надпоказателю μ и т. д. На основаніи этихъ разсужденій мы приходимъ къ заключенію, что число функцій, принадлежащихъ къ надпоказателю μ, равно одному изъ чиселъ

$$0, \mu, 2\mu, 3\mu, \ldots,$$

не превышающихъ предѣла $p^\mu - 1$. Это число можетъ быть поэтому представлено въ видѣ произведенія $\mu\theta(\mu)$, гдѣ $\theta(\mu)$ изображаетъ цѣлое число, зависящее отъ μ.

122. **Теорема.** *Число функцій, принадлежащихъ къ надпоказателю μ равно произведенію числа μ на число неприводимыхъ функцій степени μ. При этомъ предполагается, что μ есть дѣлитель степени модулярной функціи.*

На самомъ дѣлѣ, всякая функція X, удовлетворяющая сравненію

$$(1) \ldots\ldots\ldots\ldots X^{p^\mu - 1} \equiv 1, \text{ mod. } [p, F(x)]$$

принадлежитъ къ надпоказателю μ', дѣлящему число μ; ибо изъ (1) выводимъ

$$X^{p^\mu} \equiv X, \text{ mod. } [p, F(x)],$$

а отсюда заключаемъ

$$\mu \equiv 0 \text{ (mod. } \mu').$$

Обратно, всякая функція X, принадлежащая къ надпоказателю μ', равному одному изъ дѣлителей числа μ, непремѣнно удовлетворяетъ (1); ибо функція $X^{p^{\mu}-1}-1$ дѣлится тогда безъ остатка на $X^{p^{\mu'}-1}-1$.

Изображая чрезъ $\lambda, \lambda', \lambda'', \ldots$ всѣ дѣлители числа μ, на основаніи вышесказаннаго заключаемъ, что число функцій, принадлежащихъ по модулю $[p, F(x)]$ къ надпоказателямъ $\lambda, \lambda', \lambda'', \ldots$, равно числу рѣшеній сравненія (1), то есть $p^{\mu}-1$. Это можно написать такъ:

$$(2) \ldots\ldots\ldots\ldots \Sigma\lambda\theta(\lambda) = p^{\mu}-1,$$

причемъ знакъ суммы простирается на всѣ дѣлители $\lambda, \lambda', \lambda'', \ldots$ числа μ.

Изъ (2) получается общая формула для вычисленія $\theta(\mu)$. Для этого мы разлагаемъ μ на произведеніе простыхъ множителей

$$\mu = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_i^{\alpha_i},$$

и составляемъ выраженіе для $\varphi(\mu)$

$$\varphi(\mu) = \mu\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\ldots\left(1-\frac{1}{q_i}\right) = \sum\mu_1 - \sum\mu_2.$$

На основаніи извѣстной намъ теоремы имѣемъ

$$\mu\theta(\mu) = \Sigma(p^{\mu_1}-1) - \Sigma(p^{\mu_2}-1),$$

отсюда

$$(3) \ldots\ldots\ldots\ldots \theta(\mu) = \frac{\Sigma p^{\mu_1} - \Sigma p^{\mu_2}}{\mu}.$$

Сравнивая эту формулу съ (1) n^0 117 мы видимъ, что значеніе $\theta(\mu)$ равно числу функцій μ-ой степени, неприводимыхъ по модулю p. Это доказываетъ справедливость нашей теоремы.

123. **Теорема 1.** *Если по модулю $[p, F(x)]$ функція X_1 принадлежитъ къ надпоказателю μ, то наименьшій вычетъ произведенія*

$$(X-X_1)(X-X_1^{p})(X-X_1^{p^2})\ldots(X-X_1^{p^{\mu-1}})$$

представляетъ функцію μ-ой степени $f(X)$, зависящую отъ одного только перемѣннаго X, и неприводимую по модулю p.

Полагая

$$(X-X_1)(X-X_1^p)\dots(X-X_1^{p^{\mu-1}})=X^\mu-K_1X^{\mu-1}+\dots\pm K_\mu,$$

имѣемъ

$$(1)\dots\dots\dots K_i=\Sigma X_1^{p^{\alpha_1}}X_1^{p^{\alpha_2}}\dots X_1^{p^{\alpha_i}},$$

гдѣ знакъ суммы простирается на всевозможныя сочетанія $\alpha_1, \alpha_2, \dots \alpha_i$, составляемыя изъ μ элементовъ

$$0, 1, 2, \dots \mu-1$$

по i. Возвышая обѣ части (1) въ степень p, получаемъ сравненіе

$$(2)\dots K_i^p\equiv\Sigma X_1^{p^{\beta_1}}X_1^{p^{\beta_2}}\dots X_1^{p^{\beta_i}},\ \text{mod.}\ [p, F(x)],$$

гдѣ

$$\beta_1=\alpha_1+1,\ \beta_2=\alpha_2+1, \dots \beta_i=\alpha_i+1.$$

Знакъ суммы въ послѣднемъ сравненіи простирается на всѣ сочетанія $\beta_1, \beta_2, \dots \beta_i$ изъ чиселъ

$$1, 2, 3, \dots \mu,$$

по i; но такъ какъ

$$X_1^{p^\mu}\equiv X_1,\ \text{mod.}\ [p, F(x)],$$

то ясно, что на мѣсто элемента μ можно въ (2) писать нуль, вслѣдствіе чего можно прямо сказать, что знакъ суммы въ (2) простирается на всѣ сочетанія $\beta_1, \beta_2, \dots \beta_i$ изъ элементовъ

$$0, 1, 2, \dots \mu-1$$

по i. Принимая это во вниманіе, изъ (1) и (2) заключаемъ

$$K_i^p\equiv K_i,\ \text{mod.}\ [p, F(x)],$$

откуда видно, что каждый изъ коеффиціентовъ $K_1, K_2, \ldots K_\mu$ сравнимъ по модулю $[p, F(x)]$ съ однимъ изъ корней сравненія

$$X^p \equiv X, \text{ mod. } [p, F(x)],$$

то есть съ однимъ изъ чиселъ

$$0, 1, 2, \ldots p-1.$$

Слѣдовательно наименьшій вычетъ каждой изъ функцій $K_1, K_2, \ldots K_\mu$ есть *число*; а это показываетъ, что наименьшій вычетъ функціи

(3) $\ldots\ldots (X-X_1)(X-X_1^p)\ldots(X-X_1^{p^{\mu-1}}),$

взятый по модулю $[p, F(x)]$, не зависитъ отъ перемѣннаго x.

Обозначая чрезъ $f(X)$ наименьшій вычетъ произведенія (3), намъ остается теперь доказать, что по модулю p функція $f(x)$ есть неприводимая. Допустимъ противное; пусть

$$f(x) \equiv f_1(x) f_2(x) \text{ (mod. } p).$$

Функція X_1, удовлетворяя сравненію

$$f(X) \equiv 0, \text{ mod. } [p, F(x)]$$

удовлетворяетъ тѣмъ самымъ и сравненію

$$f_1(X) f_2(X) \equiv 0, \text{ mod. } [p, F(x)];$$

отсюда слѣдуетъ, что она удовлетворяетъ по крайней мѣрѣ одному изъ сравненій

(4) $\ldots\ldots\ldots f_1(X) \equiv 0, \text{ mod. } [p, F(x)],$

(5) $\ldots\ldots\ldots f_2(X) \equiv 0, \text{ mod. } [p, F(x)].$

Допустимъ, что

(6) $\ldots\ldots\ldots f_1(X_1) \equiv 0, \text{ mod. } [p, F(x)],$

и возвысимъ обѣ части сравненія (6) въ степень p^i; получаемъ

$$f_1(X_1^{p^i}) \equiv 0, \ \text{mod.}\ [p,\ F(x)].$$

Результатъ этотъ показываетъ, что функція $X_1^{p^i}$ удовлетворяетъ (4). А такъ какъ i изображаетъ произвольное число, то слѣдовательно сравненію (4) удовлетворяютъ функціи

$$X_1,\ X_1^p,\ X_1^{p^2}, \ldots X_1^{p^{\mu-1}},$$

которыя всѣ различны по модулю $[p,\ F(x)]$.

Но это невозможно, ибо степень (4) ниже μ; слѣдовательно невозможно и начальное наше предположеніе, что функція $f(x)$ разлагается по модулю p на произведеніе двухъ функцій.

Теорема 2. *Если функціи $F(x)$ и $f(x)$ неприводимы по модулю p, первая n-ой, вторая μ-ой степени, и если μ дѣлитъ n, то существуетъ такая функція X_1, принадлежащая по модулю $[p,\ F(x)]$ къ надпоказателю μ, для которой будетъ имѣть мѣсто такое тожественное сравненіе*

$$f(X) \equiv (X - X_1)(X - X_1^p)(X - X_1^{p^2}) \ldots (X - X_1^{p^{\mu-1}}),$$
$$\text{mod.}\ [p,\ F(x)].$$

Дѣйствительно, такъ какъ степень функціи $f(X)$ дѣлитъ n, то слѣдовательно $f(X)$ дѣлитъ по модулю p функцію

$$X^{p^n} - X;$$

а это показываетъ, что сравненіе

(7) . . . . $f(X) \equiv 0, \ \text{mod.}\ [p,\ F(x)]$

имѣетъ ровно μ рѣшеній.

Изображая чрезъ X_1 одно какое нибудь рѣшеніе сравненія (7), мы заключаемъ прямо, какъ при доказательствѣ предшествующей теоремы, что каждая изъ функцій въ ряду

$$X_1,\ X_1^p,\ X_1^{p^2}, \ldots X_1^{p^{\mu-1}}, \ldots$$

удовлетворяетъ (7). Отсюда слѣдуетъ, что X_1 не можетъ принадлежать къ надпоказателю большему, чѣмъ μ, ибо число корней (7) не можетъ превышать μ.

Допустимъ, что X_1 принадлежитъ къ надпоказателю $\mu' < \mu$; тогда наименьшій вычетъ произведенія

$$(X - X_1)(X - X_1^p)\dots(X - X_1^{p^{\mu'-1}})$$

представитъ функцію $f_1(X)$, μ'-ой степени и неприводимую по модулю p.

Раздѣливъ по модулю p функцію $f(X)$ на $f_1(X)$, и обозначивъ частное чрезъ Q, а остатокъ чрезъ $\varphi(X)$, будемъ имѣть тожественное сравненіе

$$(8) \dots\dots f(X) \equiv f_1(X)Q + \varphi(X) \pmod{p},$$

и сравненіе (7) можетъ быть написано такъ:

$$(9) \dots\dots f_1(X)Q + \varphi(X) \equiv 0, \text{ mod. } [p, F(x)].$$

Каждая изъ функцій въ ряду

$$X_1, X_1^p, X_1^{p^2}, \dots X_1^{p^{\mu'-1}},$$

удовлетворяя сравненію (7), тѣмъ самымъ удовлетворяетъ и (9); но онѣ очевидно удовлетворяютъ также сравненію

$$f_1(X) \equiv 0, \text{ mod. } [p, F(x)],$$

слѣдовательно онѣ удовлетворяютъ сравненію

$$\varphi(X) \equiv 0, \text{ mod. } [p, F(x)].$$

Съ другой стороны, степень функціи $\varphi(X)$ ниже μ', такъ что число рѣшеній послѣдняго сравненія превышаетъ его степень; поэтому всѣ коеффиціенты у степеней X въ выраженіи $\varphi(X)$ дѣлятся на p, и сравненіе (8) приводится къ такому

$$f(X) \equiv f_1(X)Q \pmod{p}.$$

Но это противорѣчитъ предположенію, что функція $f(x)$ неприводима по модулю p. Слѣдовательно предположеніе $\mu' < \mu$ невозможно.

Итакъ, надпоказатель, принадлежащій функціи X_1 по модулю $[p, F(x)]$, не можетъ быть ни $> \mu$, ни $< \mu$; поэтому онъ равенъ μ.

Принимая теперь во вниманіе сравненіе

$$(10)\quad f(X) \equiv (X - X_1)(X - X_1^p)(X - X_1^{p^2}) \ldots (X - X_1^{p^{\mu-1}}),\quad \text{mod. } [p, F(x)],$$

мы замѣчаемъ, что степень его ниже μ, между тѣмъ оно имѣетъ μ рѣшеній

$$X_1,\ X_1^p,\ X_1^{p^2}, \ldots X_1^{p^{\mu-1}};$$

поэтому сравненіе (10) представляетъ тожество относительно перемѣнной X. Что и требовалось доказать.

Слѣдствіе. *Сравненіе*

$$f(X) \equiv 0,\ \text{mod. } [p, F(x)]$$

имѣетъ ровно μ рѣшеній; они могутъ быть написаны такъ:

$$X_1,\ X_1^p,\ X_1^{p^2}, \ldots X_1^{p^{\mu-1}},$$

при чемъ X_1 изображаетъ одно какое нибудь изъ ихъ числа.

124. Обозначивъ, какъ выше, степень модулярной функціи $F(x)$ чрезъ n, и взявъ во вниманіе какой нибудь дѣлитель μ числа n, изобразимъ чрезъ $f(x), f_1(x), \ldots f_{r-1}(x)$ всѣ функціи μ-ой степени, неприводимыя по модулю p.

Каждое изъ сравненій

$$(1) \ldots\ldots\ldots\ldots \left.\begin{cases} f(X) \equiv 0, \\ f_1(X) \equiv 0, \\ \ldots\ldots\ldots\ldots, \\ \ldots\ldots\ldots\ldots, \\ f_{r-1}(X) \equiv 0 \end{cases}\right\} \text{mod. } [p, F(x)]$$

имѣетъ ровно μ рѣшеній, и никакое рѣшеніе не можетъ удовлетворять болѣе чѣмъ одному сравненію (1). Ибо допустивъ, что X_1 удовлетворяетъ обоимъ сравненіямъ

$$\left.\begin{aligned} f_i(X) &\equiv 0, \\ f_j(X) &\equiv 0, \end{aligned}\right\} \text{mod. } [p, F(x)],$$

мы имѣли бы тожества

$$\left.\begin{aligned} f_i(X) &\equiv (X-X_1)(X-X_1^p)\ldots(X-X_1^{p^{\mu-1}}), \\ f_j(X) &\equiv (X-X_1)(X-X_1^p)\ldots(X-X_1^{p^{\mu-1}}), \end{aligned}\right\} \text{mod. } [p, F(x)],$$

откуда вытекаетъ сравненіе

$$f_i(X) \equiv f_j(X) \ (\text{mod.}\, p),$$

показывающее, что функціи $f_i(x)$ и $f_j(x)$ тожественны по модулю p; но это противорѣчитъ предположенію, что i не равно j.

Рѣшенія сравненій (1) представляютъ функціи, принадлежащія по модулю $[p, F(x)]$ къ надпоказателю μ, и, наоборотъ, изъ теоремы 1-ой предыдущаго номера слѣдуетъ, что всякая функція, принадлежащая къ надпоказателю μ, удовлетворяетъ непремѣнно одному изъ (1). Слѣдовательно совокупность всѣхъ рѣшеній сравненій (1) представляетъ собой всѣ функціи, принадлежащія по модулю $[p, F(x)]$ къ надпоказателю μ. Отсюда прямо видно, что число функцій, принадлежащихъ къ надпоказателю μ равно μν, гдѣ ν изображаетъ число функцій μ-ой степени, неприводимыхъ по модулю p. Такимъ образомъ вновь доказана теорема n^0 122.

125. Если намъ будутъ извѣстны одна какая либо неприводимая функція $F(x)$ n-ой степени и первообразный корень A этой функціи, то тогда можно составлять прямо всѣ неприводимыя функціи, степень которыхъ дѣлитъ n, — вотъ какимъ образомъ.

Пусть μ изображаетъ какой угодно дѣлитель числа n; отыщемъ всѣ первообразные дѣлители формы $p^\mu - 1$ и обозначимъ

одинъ изъ нихъ чрезъ m. То что будетъ здѣсь сказано объ m, слѣдуетъ отнести и къ прочимъ дѣлителямъ.

Такъ какъ $p^\mu - 1$ очевидно дѣлитъ $p^n - 1$, то можно положить

$$p^n - 1 = dm.$$

Обозначая далѣе чрезъ $1, m_1, m_2, \ldots$ всѣ числа, простыя съ m и не превышающія m, и полагая

$$B \equiv A^d, \text{ mod. } [p, F(x)],$$

мы опредѣлимъ наименьшій вычетъ по модулю $[p, F(x)]$ каждой изъ функцій

$$B, B^{m_1}, B^{m_2}, \ldots$$

Получимъ такимъ образомъ $\varphi(m)$ различныхъ функцій, принадлежащихъ къ надпоказателю μ. Продѣлавъ то же самое съ прочими первообразными дѣлителями формы $p^\mu - 1$, мы будемъ имѣть всѣ функціи, принадлежащія къ надпоказателю μ.

Послѣ этого мы распредѣлимъ ихъ на группы, по μ функцій въ каждой, и, пользуясь теоремой 1-ой n^0 123, составимъ изъ каждой группы соотвѣтствующую функцію μ-ой степени, неприводимую по модулю p.

§ VII. Распредѣленіе неприводимыхъ функцій по порядкамъ. Число неприводимыхъ функцій n-ой степени и m-го порядка.

126. Извѣстно, что всякая функція $F(x)$, неприводимая по модулю p, дѣлитъ функцію

$$x^{p^n} - x,$$

гдѣ n есть степень $F(x)$. Если предположить, что функція $F(x)$ отлична отъ x, то можно сказать, что $F(x)$ дѣлитъ функцію

$$x^{p^n - 1} - 1.$$

Слѣдовательно, всегда существуетъ такое значеніе m, при которомъ функція

(1) . . . . $x^m - 1$

дѣлится по модулю p на данную неприводимую функцію $F(x)$. Особеннаго вниманія заслуживаетъ самое малое число m, при которомъ (1) дѣлится на $F(x)$; мы будемъ называть его *порядкомъ* функціи $F(x)$.

Слѣдовательно порядокъ функціи $F(x)$ есть ничто иное, какъ показатель, къ которому принадлежитъ x по модулю $[p, F(x)]$; поэтому порядокъ m функціи $F(x)$ есть первообразный дѣлитель формы $p^n - 1$ (теорема 1, n^0 120). Это, впрочемъ, легко замѣтить прямо: еслибы число m дѣлило форму $p^{n'} - 1$ при $n' < n$, то тогда функція $x^m - 1$, а тѣмъ самымъ и $F(x)$ дѣлила бы функцію $x^{p^{n'}} - 1$, что невозможно.

Порядокъ функціи вполнѣ опредѣляетъ собой ея степень, но обратно нельзя сказать.

127. Обозначивъ чрезъ m какой нибудь первообразный дѣлитель формы $p^n - 1$, мы замѣчаемъ, что въ разложеніи $x^m - 1$ на неприводимые множители по модулю p будутъ входить такія только функціи, порядокъ которыхъ дѣлитъ число m.

Дѣйствительно, положивъ

(1) . . . . $x^m - 1 \equiv V_1 V_2 \ldots V_i \pmod{p}$,

и обозначивъ чрезъ m' порядокъ какой нибудь изъ функцій V, напримѣръ V_1, имѣемъ

$$x^m - 1 \equiv 0, \text{ mod. } [p, V_1],$$
$$x^{m'} - 1 \equiv 0, \text{ mod. } [p, V_1],$$

откуда заключаемъ, что число m должно дѣлиться на m'; ибо, по модулю $[p, V_1]$, x принадлежитъ къ показателю m'.

Наоборотъ, всякая неприводимая функція V, порядокъ которой m' дѣлитъ m, содержится въ ряду $V_1, V_2, \ldots V_i$. Ибо

тогда $x^{m'}-1$ дѣлитъ x^m-1, а такъ какъ V дѣлитъ $x^{m'}-1$, то слѣдовательно V будетъ дѣлителемъ x^m-1.

Итакъ, *совокупность функцій*

$$(2) \dots\dots\dots\dots\dots V_1, V_2, \dots V_i$$

представляетъ всѣ функціи неприводимыя по модулю p, *порядокъ которыхъ есть дѣлитель числа* m.

Понятно, что степень каждой изъ функцій (2) дѣлитъ n.

Согласившись изображать чрезъ ψ_m произведеніе всѣхъ неприводимыхъ функцій m-го порядка, мы можемъ сравненіе (1) написать такъ:

$$(3) \dots\dots\dots\dots x^m-1 \equiv \Pi\psi_d \pmod{p},$$

гдѣ знакъ произведенія простирается на всѣ дѣлители d числа m.

На основаніи разсужденій подобныхъ тѣмъ, которыми мы пользовались въ n^0 114, мы имѣемъ возможность, исходя изъ (3), написать прямо выраженіе функціи ψ_m. На самомъ дѣлѣ, полагая

$$\varphi(m) = \Sigma m_1 - \Sigma m_2,$$

имѣемъ

$$(4) \dots\dots\dots\dots\dots \psi_m \equiv \frac{\Pi(x^{m_1}-1)}{\Pi(x^{m_2}-1)} \pmod{p}.$$

Здѣсь знакъ произведенія простирается: въ числителѣ на всѣ значенія m_1, а въ знаменателѣ на всѣ значенія m_2.

Функція (4) есть цѣлая, не только въ томъ случаѣ, если производить дѣленіе по модулю p, но и въ обыкновенномъ смыслѣ.

Чтобъ доказать это мы прежде всего замѣтимъ, что если какое нибудь количество x удовлетворяетъ уравненіямъ

$$x^r = 1,\ x^s = 1,$$

и притомъ s есть самое малое положительное число для котораго имѣемъ $x^s = 1$, то тогда r непремѣнно дѣлится на s. Ибо

обозначая чрезъ σ остатокъ отъ дѣленія r на s и полагая $r = sq + \sigma$, имѣемъ

$$x^{sq+\sigma} = 1,$$

что на основаніи предыдущаго уравненія приводится къ виду

$$x^{\sigma} = 1;$$

а такъ какъ $\sigma < s$, то слѣдовательно $\sigma = 0$, то есть $r = sq$.

Обозначивъ теперь чрезъ a любой корень функціи $\Pi(x^{m_2} - 1)$, мы назовемъ чрезъ s самый малый положительный показатель, при которомъ имѣетъ мѣсто уравненіе $a^s = 1$. Въ составъ каждой изъ функцій

$$\Pi(x^{m_1} - 1), \quad \Pi(x^{m_2} - 1)$$

множитель $x - a$ будетъ входить съ показателемъ равнымъ соотвѣтственно числу чиселъ m_1 или m_2, дѣлящихся на s. Но $s < m$ и потому число чиселъ, какъ перваго, такъ и втораго рода одинаково; слѣдовательно множитель $x - a$ въ выраженіи (4) сократится вполнѣ. А такъ какъ $x - a$ изображаетъ любой множитель, входящій въ составъ знаменателя формулы (4), то слѣдуетъ заключить, что формула (4) представляетъ цѣлую функцію.

128. Обозначая чрезъ ρ_m число неприводимыхъ функцій m-го порядка, и замѣчая, что степень каждой изъ такихъ функцій равна n, мы заключаемъ на основаніи выраженія функціи ψ_m,

$$(1) \ldots\ldots\ldots\ldots \rho_m = \frac{\varphi(m)}{n}.$$

Формула эта даетъ возможность узнать на сколько неприводимыхъ множителей разлагается функція

$$(2) \ldots\ldots\ldots\ldots \psi_m = \frac{\Pi(x^{m_1} - 1)}{\Pi(x^{m_2} - 1)},$$

по данному модулю p, простому съ m.

Какъ слѣдствіе изъ (1) вытекаетъ слѣдующее предложеніе.

Чтобы функція

$$\frac{\Pi(x^{m_1}-1)}{\Pi(x^{m_2}-1)}$$

была неприводимою по модулю p, простомъ съ m, необходимо и достаточно, чтобъ p было первообразнымъ корнемъ числа m.

Отсюда слѣдуетъ, что если число m не имѣетъ первообразнаго корня, то функція (2) будетъ приводимою относительно всякаго модуля p, не дѣлящаго m.

129. Въ частномъ случаѣ, когда m дѣлится на p, функція ψ_m теряетъ прежній смыслъ. Посмотримъ, что она будетъ тогда представлять.

Положивъ

$$(1) \ldots\ldots\ldots\ldots\ldots \quad m = m'p^\alpha,$$

причемъ m' не дѣлится на p, и опредѣливъ числа m'_1 и m'_2 по формулѣ

$$(2) \ldots\ldots\ldots\ldots \quad \varphi(m') = \Sigma m'_1 - \Sigma m'_2,$$

мы возьмемъ во вниманіе функцію

$$(3) \ldots\ldots\ldots\ldots \quad \psi_{m'} = \frac{\Pi(x^{m'_1}-1)}{\Pi(x^{m'_2}-1)},$$

которая по модулю p представляетъ произведеніе всѣхъ неприводимыхъ функцій m'-го порядка.

Имѣемъ

$$\psi_{m'}^{p^{\alpha-1}(p-1)} = \frac{\Pi(x^{m'_1}-1)^{p^\alpha}\,\Pi(x^{m'_2}-1)^{p^{\alpha-1}}}{\Pi(x^{m'_1}-1)^{p^{\alpha-1}}\,\Pi(x^{m'_2}-1)^{p^\alpha}},$$

что на основаніи извѣстной теоремы приводитъ къ слѣдующему тожественному сравненію:

$$(4) \ldots \quad \psi_{m'}^{p^{\alpha-1}(p-1)} \equiv \frac{\Pi(x^{m'_1 p^\alpha}-1)\,\Pi(x^{m'_2 p^{\alpha-1}}-1)}{\Pi(x^{m'_1 p^{\alpha-1}}-1)\,\Pi(x^{m'_2 p^\alpha}-1)} \pmod{p}.$$

Съ другой стороны, полагая

$$\varphi(m) = \Sigma m_1 - \Sigma m_2,$$

изъ (1) и (2) получаемъ для опредѣленія совокупности чиселъ m_1 и m_2 такія формулы:

$$\Sigma m_1 = \Sigma m'_1 p^\alpha + \Sigma m'_2 p^{\alpha-1},$$
$$\Sigma m_2 = \Sigma m'_1 p^{\alpha-1} + \Sigma m'_2 p^\alpha.$$

Отсюда заключаемъ, что формулу (4) можно написать такъ:

$$\psi_{m'}^{p^{\alpha-1}(p-1)} \equiv \frac{\Pi(x^{m_1}-1)}{\Pi(x^{m_2}-1)} \pmod{p}$$

или, что одно и тоже,

(5) . . . . $\psi_m \equiv \psi_{m'}^{p^{\alpha-1}(p-1)} \pmod{p}$.

Эта формула даетъ искомое разложеніе функціи ψ_m. Отсюда слѣдуетъ, что *для того, чтобы функція* ψ_m *была неприводима по модулю* p, *дѣлящему* m, *необходимы и достаточны два условія:*

1°. $p = 2$, $\alpha = 1$;

2°. *модуль* 2 *долженъ быть первообразнымъ корнемъ числа* m'.

Принимая во вниманіе послѣднія условія и то, что было сказано ранѣе о функціи ψ_m, мы заключаемъ, что *если* m *не имѣетъ первообразныхъ корней, то функція* ψ_m *есть всегда приводимая, каковъ бы ни былъ модуль* p.

130. *Примѣръ.* Опредѣлимъ порядокъ и число неприводимыхъ функцій разныхъ порядковъ въ нѣсколькихъ простѣйшихъ частныхъ предположеніяхъ, относящихся къ модулю p и къ степени n.

1°. $p = 2$, $n = 2$. Въ этомъ случаѣ форма $2^2 - 1 = 3$ имѣетъ одинъ только первообразный дѣлитель, именно 3.

Число неприводимыхъ функцій третьяго порядка есть

$$\rho_3 = \frac{\varphi(3)}{2} = 1.$$

Слѣдовательно въ разсматриваемомъ случаѣ существуетъ одна только неприводимая функція; она есть третьяго порядка и опредѣляется по формулѣ

$$\psi_3 = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

2°. $p = 2$, $n = 3$. Форма $2^3 - 1 = 7$ имѣетъ одинъ только первообразный дѣлитель, именно 7. Число неприводимыхъ функцій седьмаго порядка есть

$$\rho_7 = \frac{\varphi(7)}{3} = 2;$$

слѣдовательно существуетъ всего только двѣ неприводимыя функціи; обѣ онѣ седьмаго порядка.

3°. $p = 2$, $n = 4$. Первообразные дѣлители формы $2^4 - 1 = 15$ суть 5 и 15. Имѣемъ

$$\rho_5 = \frac{\varphi(5)}{4} = 1,$$

$$\rho_{15} = \frac{\varphi(15)}{4} = 2.$$

Число всѣхъ неприводимыхъ функцій равно 3. Одна только изъ ихъ числа есть пятаго порядка, именно:

$$\psi_5 = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + 1.$$

4°. $p = 2$, $n = 5$. Форма $2^5 - 1 = 31$ имѣетъ одинъ только первообразный дѣлитель 31, слѣдовательно всѣ неприводимыя функціи суть 31-го порядка; ихъ число равно

$$\rho_{31} = \frac{\varphi(31)}{5} = 6.$$

5°. $p = 2$, $n = 6$. Первообразные дѣлители формы $2^6 - 1 = 63$ суть 9, 21, 63; находимъ

$$\rho_9 = 1, \ \rho_{21} = 2, \ \rho_{63} = 6.$$

Всѣхъ неприводимыхъ формъ существуетъ слѣдовательно 9; изъ нихъ одна только девятаго порядка, именно:

$$\psi_9 = \frac{x^9-1}{x^3-1} = x^6 + x^3 + 1.$$

Всего болѣе вниманія заслуживаетъ тотъ первообразный дѣлитель формы $p^n - 1$, которому соотвѣтствуетъ наименьшее значеніе ρ_m. Эти минима, въ простѣйшихъ предположеніяхъ относительно p и n, суть слѣдующіе:

$p = 2.$

$n = 2,$	$\rho_3 = 1;$	$n = 7,$	$\rho_{127} = 18;$
$n = 3,$	$\rho_7 = 2;$	$n = 8,$	$\rho_{17} = 2;$
$n = 4,$	$\rho_5 = 1;$	$n = 9,$	$\rho_{73} = 8;$
$n = 5,$	$\rho_{31} = 6;$	$n = 10,$	$\rho_{11} = 1;$
$n = 6,$	$\rho_9 = 1;$	$n = 11,$	$\rho_{23} = 2.$

$p = 3.$

$n = 2,$	$\rho_4 = 1;$	$n = 6,$	$\rho_7 = 1;$
$n = 3,$	$\rho_{13} = 4;$	$n = 7,$	$\rho_{1093} = 156;$
$n = 4,$	$\rho_5 = 1;$	$n = 8,$	$\rho_{32} = 2;$
$n = 5,$	$\rho_{11} = 2;$	$n = 9,$	$\rho_{757} = 84.$

$p = 5.$

$n = 2,$	$\rho_3 = 1;$	$n = 6,$	$\rho_7 = 1;$
$n = 3,$	$\rho_{31} = 10;$	$n = 7,$	$\rho_{19530} = 2790;$
$n = 4,$	$\rho_{16} = 2;$	$n = 8,$	$\rho_{32} = 2;$
$n = 5,$	$\rho_{11} = 2;$	$n = 9,$	$\rho_{19} = 2.$

$p = 7.$

$n = 2,$	$\rho_4 = 1;$	$n = 6,$	$\rho_{36} = 2;$
$n = 3,$	$\rho_9 = 2;$	$n = 7,$	$\rho_{4733} = 676;$
$n = 4,$	$\rho_5 = 1;$	$n = 8,$	$\rho_{64} = 4;$
$n = 5,$	$\rho_{2801} = 560;$	$n = 9,$	$\rho_{27} = 2.$

$$p = 11.$$

$n = 2,$	$\rho_3 = 1;$	$n = 6,$	$\rho_9 = 1;$
$n = 3,$	$\rho_7 = 2;$	$n = 7,$	$\rho_{43} = 6;$
$n = 4,$	$\rho_{16} = 2;$	$n = 8,$	$\rho_{32} = 2;$
$n = 5,$	$\rho_{25} = 4;$	$n = 9,$	$\rho_{1772893} = 196988.$

Во многихъ частныхъ случаяхъ подобныя таблицы значительно облегчаютъ отыскиванiе неприводимыхъ функцiй.

ГЛАВА X.

О функціяхъ абсолютно неприводимыхъ.

§ I. Начала дѣлимости.

131. Дѣлимость функціи $f(x)$ на $\varphi(x)$ обусловливается равенствомъ

$$f(x) = \varphi(x)\, \psi(x),$$

причемъ функція $\psi(x)$ должна быть цѣлой.

Если $\varphi(x)$ дѣлитъ $f(x)$, то $A\varphi(x)$ дѣлитъ очевидно $Bf(x)$, каковы бы ни были числовые коеффиціенты A и B; слѣдовательно, по отношенію къ дѣлимости, функціи, отличающіяся постоянными множителями, можно не считать за различныя, и если ограничиться функціями съ коеффиціентами исключительно раціональными, то можно предполагать, что въ дѣлимомъ, какъ и въ дѣлителѣ, коеффиціенты суть цѣлыя числа, не имѣющія общаго дѣлителя.

Функцію съ цѣлыми коеффиціентами, не имѣющими общаго дѣлителя, согласимся называть *несократимою*.

Можно разсматривать единицу, какъ несократимую функцію нулевой степени.

Теорема. *Произведеніе двухъ несократимыхъ функцій есть функція также несократимая.*

На самомъ дѣлѣ, допустимъ противное; пусть $\varphi(x)$ и $\psi(x)$ будутъ несократимыми функціями, и пусть всѣ коэффиціенты въ произведеніи $\varphi(x)\,\psi(x)$ дѣлятся на простое число p; тогда будемъ имѣть сравненіе

$$\varphi(x)\,\psi(x) \equiv 0 \pmod{p},$$

откуда заключаемъ (n^0 71), что по крайней мѣрѣ одна изъ функцій $\varphi(x)$ и $\psi(x)$ сравнима съ нулемъ по модулю p. Но это противорѣчитъ предположенію, что обѣ функціи $\varphi(x)$ и $\psi(x)$ суть несократимыя; слѣдовательно, общій наибольшій дѣлитель всѣхъ коэффиціентовъ въ произведеніи $\varphi(x)\,\psi(x)$ равенъ единицѣ.

Слѣдствіе. *Если несократимая функція $f(x)$ дѣлится на несократимую функцію $\varphi(x)$, то частное есть функція также несократимая.*

Дѣйствительно, частное отъ дѣленія $f(x)$ на $\varphi(x)$ можно представить въ видѣ $\frac{m}{n}\psi(x)$, причемъ $\psi(x)$ изображаетъ несократимую функцію, а m и n цѣлыя числа. Полагая

$$F(x) = nf(x) = m\varphi(x)\,\psi(x),$$

мы заключаемъ, что общій наибольшій дѣлитель всѣхъ коэффиціентовъ въ выраженіи функціи $F(x)$ равенъ разъ числу n, другой разъ числу m; слѣдовательно $n = m$, и потому частное отъ дѣленія $f(x)$ на $\varphi(x)$ равно несократимой функціи $\psi(x)$.

132. По извѣстному способу Эвклида, понятіе объ общемъ наибольшемъ дѣлителѣ, равно какъ и основныя свойства функцій взаимно простыхъ, устанавливаются безразлично, какъ для функцій съ какими угодно коэффиціентами, такъ и для функцій съ цѣлыми коэффиціентами; но что касается разложенія функцій на множители, то вопросъ этотъ представляется въ совершенно иномъ видѣ, смотря по тому будемъ ли мы обращать вниманіе на натуру коэффиціентовъ, или не будемъ. Такъ, напримѣръ, всякая функція имѣетъ линейный дѣлитель $x + a$, но если мы

поставимъ условіе, что a должно быть числомъ цѣлымъ, то тогда можетъ не оказаться ни одного дѣлителя означеннаго вида.

Не желая выходить здѣсь изъ области цѣлыхъ чиселъ, мы ограничимся исключительно функціями съ цѣлыми коеффиціентами, подразумѣвая постоянно, что въ кругу нашихъ изысканій всякая функція есть несократимая. Имѣя это въ виду, мы согласимся называть функцію P *абсолютно неприводимою*, или просто *неприводимою*, если она не имѣетъ никакихъ другихъ дѣлителей кромѣ 1 и P. Такія функціи играютъ ту же роль въ области цѣлыхъ функцій съ цѣлыми коеффиціентами, что простыя числа въ области всѣхъ цѣлыхъ чиселъ.

Если неприводимая функція P не дѣлитъ $f(x)$, то P и $f(x)$ суть взаимно простыя.

Если неприводимая функція P дѣлитъ произведеніе нѣсколькихъ функцій $f_1(x)\ f_2(x)\ f_3(x) \ldots$, то она дѣлитъ по крайней мѣрѣ одинъ изъ множителей $f_1(x)$, $f_2(x), \ldots$

Всякая функція $f(x)$ или сама есть неприводимая, или разлагается на произведеніе нѣсколькихъ неприводимыхъ множителей; такое разложеніе возможно однимъ только образомъ.

Число неприводимыхъ функцій безконечно.

Всѣ эти предложенія доказываются также, какъ и для цѣлыхъ чиселъ.

133. Разложеніе функціи $f(x)$ на неприводимые множители можетъ быть выполнено съ помощью конечнаго числа испытаній. Это ясно видно изъ того, что числовыя величины коеффиціентовъ въ искомомъ дѣлителѣ, степень котораго задана напередъ, не превосходятъ извѣстныхъ предѣловъ, зависящихъ отъ высшаго предѣла модулей всѣхъ корней функціи $f(x)$. Вслѣдствіе этого получаемъ для искомаго дѣлителя конечное число возможныхъ выраженій, которыя подвергая поочередно испытанію, мы опредѣлимъ всѣ дѣлители заданной степени, или убѣдимся окончательно, что подобныхъ дѣлителей вовсе не существуетъ.

При отыскиваніи дѣлителей слѣдуетъ начинать съ дѣлителей первой степени, а если таковыхъ не окажется, перейти къ оты-

скиванію дѣлителей второй степени и т. д. Если окажется, что $f(x)$ не имѣетъ ни одного дѣлителя степени $\leqq \frac{n}{2}$, то тогда слѣдуетъ заключить, что функція $f(x)$ неприводима.

Дѣлитель возможно низкой степени есть всегда функція неприводимая.

Понятно, что, зная дѣлитель функціи

$$f(x) = px^n + p_1 x^{n-1} + \ldots + p_n,$$

мы тѣмъ самымъ знаемъ дѣлитель функціи

$$p^{n-1} f\left(\frac{x}{p}\right) = x^n + p_1 x^{n-1} + \ldots + p_n p^{n-1},$$

и наоборотъ; поэтому всегда можно предположить, что функція, которую требуется разложить на множители, имѣетъ коеффиціентъ у наивысшей степени перемѣннаго равный единицѣ.

134. Для отысканія дѣлителей функціи $f(x)$ можно поступать по указанію Кронекера еще слѣдующимъ образомъ.

Пусть m изображаетъ степень искомаго дѣлителя $\varphi(x)$.

Возьмемъ $m+1$ частныхъ значеній для x

$$x = a_0, a_1, \ldots a_m,$$

разумѣется цѣлыхъ, и вычислимъ соотвѣтствующія значенія

$$f(x) = b_0, b_1, \ldots b_m,$$

которыя очевидно будутъ также цѣлыми.

Значенія

$$\varphi(x) = u_0, u_1, \ldots u_m$$

будутъ также цѣлыми, но при этомъ u_0 должно дѣлить b_0, u_1 должно дѣлить b_1 и т. д.; слѣдовательно каждое изъ чиселъ $u_0, u_1, \ldots$ можетъ имѣть одно изъ нѣсколькихъ заранѣе опредѣляемыхъ значеній. Но числа $u_0, u_1, \ldots$ вполнѣ опредѣляютъ собой функцію $\varphi(x)$; поэтому можно всегда напередъ составить извѣстное число выраженій, единственно возможныхъ для $\varphi(x)$.

Испытывая каждое изъ нихъ поочередно, мы такимъ образомъ отыщемъ всѣ дѣлители степени не выше m или убѣдимся, что таковыхъ не существуетъ вовсе.

135. Остатокъ отъ дѣленія функціи

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_n$$

на

$$\varphi(x) = x^m + a_1 x^{m-1} + \ldots + a_m$$

представляется въ видѣ функціи $(m-1)$-ой степени, въ которой коэффиціенты суть функціи чиселъ $a_1, a_2, \ldots a_m$. Приравнивъ эти коэффиціенты нулю, мы получимъ m уравненій съ m неизвѣстными цѣлыми числами $a_1, a_2, \ldots a_m$; это будутъ условія дѣлимости $f(x)$ на $\varphi(x)$.

Рѣшеніе нѣсколькихъ уравненій съ нѣсколькими неизвѣстными при помощи послѣдовательныхъ исключеній приводится къ рѣшенію одного уравненія съ одною неизвѣстной; поэтому вопросъ объ отысканіи дѣлителей функціи можно окончательно свести на рѣшеніе въ цѣлыхъ числахъ одного уравненія съ одною неизвѣстной.

Въ частномъ случаѣ, когда идетъ дѣло объ отысканіи квадратичныхъ дѣлителей, мы будемъ имѣть первоначально два уравненія съ двумя неизвѣстными

$$\varphi_1(a_1, a_2) = 0, \quad \varphi_2(a_1, a_2) = 0,$$

притомъ a_2 должно дѣлить p_n. Приравнивая послѣдовательно неизвѣстное a_2 разнымъ дѣлителямъ числа p_n, мы будемъ получать каждый разъ по два уравненія съ однимъ неизвѣстнымъ a_1, и если окажется общее цѣлое рѣшеніе, то получимъ тогда и общій квадратичный дѣлитель.

136. *Примѣръ 1. Найти квадратичные дѣлители функціи*

$$f(x) = x^4 + p_1 x^3 + p_2 x^2 + p_3 x + p_4.$$

Изображая искомый дѣлитель чрезъ

$$\varphi(x) = x^2 + ax + b,$$

имѣемъ

$$\left.\begin{aligned} x^2 &\equiv -ax-b, \\ x^3 &\equiv (a^2-b)\,x+ab, \\ x^4 &\equiv a(2b-a^2)\,x+b(b-a^2), \end{aligned}\right\}\ [\text{mod. } \varphi(x)].$$

Слѣдовательно, отъ дѣленія $f(x)$ на $\varphi(x)$ получается остатокъ

$$[a(2b-a^2)+(a^2-b)\,p_1-ap_2+p_3]\,x+b(b-a^2) \\ +abp_1-bp_2+p_4;$$

отсюда два уравненія для опредѣленія a и b, именно:

$$(1)\ \ldots\ldots \begin{cases} a(2b-a^2)+(a^2-b)\,p_1-ap_2+p_3=0, \\ b(b-a^2)+abp_1-bp_2+p_4=0. \end{cases}$$

Изъ послѣдняго видно, что b должно дѣлить p_4. Приравнивая b какому нибудь дѣлителю числа p_4 и полагая

$$(2)\ \ldots\ldots\ldots\ldots\ldots\ldots\ p_4=bb',$$

на мѣсто (1) имѣемъ

$$(3)\ \ldots\ldots \begin{cases} a(2b-a^2)+(a^2-b)\,p_1-ap_2+p_3=0, \\ b-a^2+ap_1-p_2+b'=0; \end{cases}$$

отсюда выводимъ

$$ab-bp_1+p_3-ab'=0;$$

слѣдовательно, на мѣсто (3) имѣемъ

$$(4)\ \ldots\ldots\ldots\ldots \begin{cases} p_3-bp_1=a(b'-b), \\ p_2-b-b'=a(p_1-a). \end{cases}$$

Первое изъ этихъ уравненій показываетъ, что p_3-bp_1 должно дѣлиться на $b'-b$; въ противномъ случаѣ принятое значеніе для b не годится.

Если $p_3 - bp_1$ дѣлится на самомъ дѣлѣ на $b' - b$, то тогда имѣемъ

(5) . . . . $a = \frac{p_3 - bp_1}{b' - b}$,

и смотря по тому будетъ ли значеніе (5) удовлетворять второму уравненію (4), или не будетъ, функція $x^2 + ax + b$ будетъ дѣлить $f(x)$, или не будетъ.

Если $b' = b$, въ такомъ случаѣ должно имѣть мѣсто уравненіе $p_3 = bp_1$; иначе значеніе, принятое для b, не годится. Допустивъ, что дѣйствительно $p_3 = bp_1$, для опредѣленія a имѣемъ уравненіе

$$a^2 - p_1 a + p_2 - 2b = 0;$$

если оно не будетъ имѣть цѣлыхъ рѣшеній, тогда значеніе, принятое для b, не годится.

137. *Примѣръ 2. Найти кубичный дѣлитель функціи*

$$x^6 + p_1 x^5 + p_2 x^4 + \ldots + p_6.$$

Изобразивъ искомый дѣлитель чрезъ

$$\varphi(x) = x^3 - ax^2 - bx - c,$$

можемъ написать

$$\left.\begin{aligned} x^3 &\equiv ax^2 + bx + c, \\ x^4 &\equiv a_1 x^2 + b_1 x + c_1, \\ x^5 &\equiv a_2 x^2 + b_2 x + c_2, \\ x^6 &\equiv a_3 x^2 + b_3 x + c_3, \end{aligned}\right\} [\text{mod. } \varphi(x)],$$

гдѣ $a_1, b_1, \ldots c_3$ вычисляются по формуламъ

$$a_n = aa_{n-1} + b_{n-1},$$
$$b_n = ba_{n-1} + c_{n-1},$$
$$c_n = ca_{n-1},$$

если полагать послѣдовательно $n = 1, 2, 3$.

Условія дѣлимости данной функціи на $\varphi(x)$ выражаются уравненіями

$$(1) \ldots\ldots \begin{cases} a_3 + p_1 a_2 + p_2 a_1 + p_3 a + p_4 = 0, \\ b_3 + p_1 b_2 + p_2 b_1 + p_3 b + p_5 = 0, \\ c_3 + p_1 c_2 + p_2 c_1 + p_3 c + p_6 = 0. \end{cases}$$

Изъ послѣдняго уравненія (1), подставляя въ немъ на мѣсто c_3, c_2, c_1 значенія

$$c_3 = ca_2, \quad c_2 = ca_1, \quad c_1 = ca,$$

выводимъ

$$c(a_2 + p_1 a_1 + p_2 a + p_3) + p_6 = 0;$$

отсюда заключаемъ, что c дѣлитъ p_6.

Приравнивъ c какому нибудь дѣлителю числа p_6, будемъ имѣть

$$(2) \ldots\ldots\ldots\ldots\ldots \; p_6 = cc',$$

$$(3) \ldots\ldots\ldots \; a_2 + p_1 a_1 + p_2 a + p_3 + c' = 0.$$

Исключая съ помощью уравненія (3) величину p_3 изъ первыхъ двухъ уравненій (1), получаемъ

$$(4) \ldots\ldots\ldots \begin{cases} b_2 + p_1 b_1 + p_2 b + p_4 - ac' = 0, \\ c_2 + p_1 c_1 + p_2 c + p_5 - bc' = 0. \end{cases}$$

На мѣсто условій (1) мы имѣемъ теперь уравненія (3) и (4).

Внося въ послѣднее уравненіе (4) на мѣсто c_2 и c_1 значенія ca_1 и ca, получаемъ

$$(5) \ldots\ldots\ldots \; c(a_1 + p_1 a + p_2) + p_5 - bc' = 0.$$

Отсюда слѣдуетъ, что *общій наибольшій дѣлитель чиселъ c и c' долженъ дѣлить p_5*; въ противномъ случаѣ, принятое значеніе для c слѣдуетъ покинуть.

Обозначивъ чрезъ d общій наибольшій дѣлитель чиселъ c и c', мы положимъ

(6) . . . . $c = dd',\quad c' = dd'',\quad p_5 = dq.$

Уравненіе (5) принимаетъ вслѣдствіе этого такой видъ:

(7) . . . . $d'(a_1 + p_1 a + p_2) + q - bd'' = 0.$

Отсюда слѣдуетъ, что b удовлетворяетъ сравненію

(8) . . . . $d''x \equiv q \pmod{d'},$

и если обозначимъ чрезъ α какое нибудь его рѣшеніе, то можемъ написать

(9) . . . . $b = \alpha - d't,$

гдѣ t изображаетъ новое неизвѣстное цѣлое число, которое мы введемъ на мѣсто b.

Внося въ (7) на мѣсто b выраженіе (9) и полагая для сокращенія

(10) . . . . $q - \alpha d'' = d'f,$

получаемъ

(11) . . . . . . $a_1 + p_1 a + p_2 + f + d''t = 0.$

Исключая съ помощью этого уравненія величину p_2 изъ (3) и перваго (4), получаемъ

(12) . . . . $\begin{cases} b_1 + p_1 b + p_3 + c' - a(f + d''t) = 0, \\ c_1 + p_1 c + p_4 - ac' - b(f + d''t) = 0. \end{cases}$

На мѣсто условій (1) имѣемъ теперь уравненія (11) и (12).

Внося во второе (12) ac на мѣсто c_1 и $\alpha - d't$ на мѣсто b, получаемъ

(13) . . . $a(c - c') = (\alpha - d't)(f + d''t) - p_1 c - p_4,$

откуда заключаемъ, что искомое число t должно удовлетворять сравненію второй степени

$$(14) \ldots (a - d't)(f + d''t) \equiv p_4 + p_1 c \ [\text{mod.}\ (c - c')].$$

Въ случаѣ, если сравненіе это окажется невозможнымъ, принятое значеніе для c надо перемѣнить на другое.

Допустимъ, что сравненіе (14) возможно, и обозначимъ чрезъ β одинъ какой нибудь его корень; число значеній β равно числу различныхъ рѣшеній сравненія (14).

Число t можетъ быть представлено въ видѣ

$$(15) \ldots\ldots\ldots\ldots t = \beta - (c - c')u,$$

причемъ u изображаетъ новое неизвѣстное цѣлое число.

Внося въ (13) на мѣсто t его выраженіе по послѣдней формулѣ, и, затѣмъ, сокращая обѣ части на $c - c'$, получаемъ

$$(16) \ldots\ldots\ldots\ldots a = h + h'u + h''u^2,$$

гдѣ h, h', h'' изображаютъ извѣстныя цѣлыя числа.

Подобнымъ образомъ изъ (9) выводимъ

$$(17) \ldots\ldots\ldots\ldots b = k + k'u,$$

гдѣ k и k' изображаютъ извѣстныя цѣлыя числа.

Наша задача сведена теперь къ опредѣленію одного u; по немъ коеффиціенты a и b опредѣляются непосредственно.

Внося въ уравненіе (11) и въ первое (12) на мѣсто a, b, t соотвѣтствующія выраженія по формуламъ (15), (16), (17), причемъ на мѣсто a_1 и b_1 слѣдуетъ подставить предварительно ихъ значенія

$$a_1 = a^2 + b, \quad b_1 = ab + c,$$

мы получимъ два уравненія третьей и четвертой степени съ однимъ неизвѣстнымъ u. Если они имѣютъ общій цѣлый корень, тогда по этому корню мы вычислимъ a и b и получимъ искомый

дѣлитель $\varphi(x)$; въ противномъ случаѣ слѣдуетъ мѣнять значенія β и c. Если при всевозможныхъ значеніяхъ для c и для β не получится дѣлитель, то слѣдуетъ тогда заключить, что заданная функція вовсе не имѣетъ кубическихъ дѣлителей.

Остается еще обратить вниманіе на частный случай, когда $c = c'$. Тогда имѣемъ

$$d = c,\ d' = d'' = 1,\ p_5 = cq,\ \alpha = q,\ f = 0,\ b = q - t;$$

уравненія (11) и (12) представляются въ слѣдующемъ видѣ:

$$t^2 - qt + p_1 c + p_4 = 0,$$
$$a^2 + p_1 a + q + p_2 = 0,$$
$$a(q - 2t) + p_1(q - t) + 2c + p_3 = 0.$$

Если два первыя изъ числа этихъ уравненій имѣютъ цѣлые корни, и эти корни удовлетворяютъ послѣднему уравненію, тогда получимъ кубичный дѣлитель заданной функціи.

Примѣчаніе. Способы, изложенные нами въ двухъ послѣднихъ примѣрахъ, примѣняются къ функціямъ какой угодно степени.

§ II. Доказательство одного сравненія.

138. **Теорема.** *Если функціи $F(x)$ и $F_1(x)$ сравнимы по модулю p, то ихъ результанты, составленные относительно одной и той же функціи вида*

$$x^n + p_1 x^{n-1} + \ldots + p_n,$$

также сравнимы по модулю p.

Дѣйствительно, двѣ функціи, сравнимыя по модулю p, отъ дѣленія на функцію вида

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_n$$

даютъ въ остаткѣ, равно какъ и въ частномъ, функціи, соотвѣтственно сравнимыя по модулю p.

Изображая соотвѣтственно чрезъ

$$a_0^{(i)} + a_1^{(i)}x + \ldots + a_{n-1}^{(i)}x^{n-1},$$
$$b_0^{(i)} + b_1^{(i)}x + \ldots + b_{n-1}^{(i)}x^{n-1}$$

остатки получаемые отъ дѣленія функцій

$$x^i F(x) \quad \text{и} \quad x^i F_1(x)$$

на $f(x)$ и замѣчая, что

$$x^i F(x) \equiv x^i F_1(x) \pmod{p},$$

мы имѣемъ рядъ сравненій

$$\left.\begin{array}{c} a_0^{(i)} \equiv b_0^{(i)}, \\ a_1^{(i)} \equiv b_1^{(i)}, \\ \cdots\cdots\cdots \\ \cdots\cdots\cdots \\ a_{n-i}^{(i)} \equiv b_{n-1}^{(i)} \end{array}\right\} \pmod{p},$$

при всякомъ i, начиная съ $i = 0$.

Съ другой стороны, обозначая соотвѣтственно чрезъ R и R_1 результанты функцій $F(x)$ и $F_1(x)$, составленные относительно $f(x)$, имѣемъ

$$R = \begin{vmatrix} a_0 \; a_1 \ldots a_{n-1} \\ a'_0 \; a'_1 \ldots a'_{n-1} \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ a_0^{(n-1)} \; a_1^{(n-1)} \ldots a_{n-1}^{(n-1)} \end{vmatrix},$$

$$R_1 = \begin{vmatrix} b_0 \; b_1 \ldots b_{n-1} \\ b'_0 \; b'_1 \ldots b'_{n-1} \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ b_0^{(n-1)} \; b_1^{(n-1)} \ldots b_{n-1}^{(n-1)} \end{vmatrix}.$$

Отсюда, на основаніи предыдущихъ сравненій, непосредственно заключаемъ

$$R \equiv R_1 \pmod{p},$$

что и слѣдовало доказать.

139. Прослѣдивъ ходъ доказательства послѣдней теоремы, легко замѣтить, что она остается въ силѣ и въ томъ случаѣ, когда коеффиціенты въ выраженіяхъ функцій $f(x)$, $F(x)$, $F_1(x)$ содержатъ произвольный параметръ y, представляясь въ видѣ цѣлыхъ функцій этого параметра. Разсматривая тогда y какъ перемѣнную, сравненіе

$$(1) \ldots\ldots\ldots\ldots R \equiv R_1 \pmod{p}$$

будетъ представлять тожественное функціональное сравненіе.

Вообще, функціи $f(x)$, $F(x)$, $F_1(x)$ могутъ содержать какое угодно число независимыхъ параметровъ и всегда сравненіе (1) остается справедливымъ.

Переходя къ приложенію предыдущаго, мы докажемъ слѣдующую теорему Шенемана.

Теорема. *Каково бы ни было простое число p, если функціи*

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_n,$$
$$\Phi(x) = x^n + q_1 x^{n-1} + \ldots + q_n$$

таковы, что корни второй равны p-ой степени отъ корней первой, то такія функціи сравнимы по модулю p.

Дѣйствительно, разсматривая X какъ произвольный параметръ и замѣчая, что функціи

$$(X-x)^p \quad \text{и} \quad X^p - x^p$$

сравнимы по модулю p, имѣемъ сравненіе

$$(X-x_1)^p(X-x_2)^p\ldots(X-x_n)^p \equiv (X^p-x_1^p)(X^p-x_2^p)\ldots(X^p-x_n^p),$$

причемъ $x_1, x_2, \ldots x_n$ изображаютъ корни функціи $f(x)$.

Сравненіе это можно написать проще такъ:

$$(2) \ldots\ldots\ldots\ldots \quad f(X)^p \equiv \Phi(X^p) \pmod{p}.$$

Съ другой стороны, по извѣстной теоремѣ имѣемъ

$$(3) \ldots\ldots\ldots\ldots \quad f(X)^p \equiv f(X^p) \pmod{p}.$$

Изъ (2) и (3) выводимъ

$$f(X^p) \equiv \Phi(X^p) \pmod{p}.$$

Отсюда, внося въ обѣ части x на мѣсто X^p, получаемъ

$$f(x) \equiv \Phi(x) \pmod{p},$$

что и слѣдовало доказать.

Примѣръ. Возьмемъ уравненіе

$$x^3 - x + 1 = 0,$$

и положимъ

$$y = x^7.$$

Составляемъ рядъ уравненій

$$y = -1 + 2x - 2x^2,$$

$$xy = 2 - 3x + 2x^2,$$

$$x^2 y = -2 + 4x - 3x^2,$$

откуда выводимъ

$$\begin{vmatrix} -1-y & 2 & -2 \\ 2 & -3-y & 2 \\ -2 & 4 & -3-y \end{vmatrix} = 0.$$

Разлагая опредѣлитель, получаемъ уравненіе

$$y^3 + 7y^2 - y + 1 = 0. \ldots$$

Полагая

$$f(x) = x^3 - x + 1,$$

$$\Phi(x) = x^3 + 7x^2 - x + 1,$$

мы убѣждаемся въ справедливости сравненія

$$f(x) \equiv \Phi(x) \pmod{7}.$$

§ III. Разложеніе функціи $x^m - 1$ на неприводимые множители.

140. Изображая чрезъ ψ_m произведеніе всѣхъ неприводимыхъ функцій m-го порядка по модулю p, мы имѣемъ слѣдующее разложеніе функціи $x^m - 1$ на множители (n^0 127)

$$(1) \; \ldots\ldots\ldots \; x^m - 1 \equiv \psi_m \psi_{m'} \ldots \psi_1 \pmod{p}$$

гдѣ m, m', ... 1 означаютъ различные дѣлители числа m.

Функція ψ_m составляется по формулѣ

$$(2) \; \ldots\ldots\ldots \; \psi_m = \frac{\Pi(x^{m_1} - 1)}{\Pi(x^{m_2} - 1)},$$

причемъ совокупность чиселъ m_1 и m_2 находится изъ выраженія

$$\varphi(m) = \Sigma m_1 - \Sigma m_2.$$

Сравненіе (1) не нарушается, если во второй его части на мѣсто какой нибудь изъ функцій ψ подставить другую, сравнимую съ первой по модулю p; но если подъ знакомъ ψ_m понимать точно выраженіе (2), то тогда сравненіе (1) превращается въ уравненіе (n^0 14)

$$(3) \; \ldots\ldots\ldots \; x^m - 1 = \psi_m \psi_{m'} \ldots \psi_1.$$

Характеристическое свойство функціи (2) состоитъ въ томъ, что при всякомъ m она абсолютно неприводима; такъ что равен-

ство (3) представляетъ разложеніе функціи $x^m - 1$ на абсолютно неприводимые множители.

Прежде чѣмъ доказать это, мы, слѣдуя Дедекинду, укажемъ на особенности корней функціи ψ_m.

141. Корни двучленнаго уравненія $x^m - 1 = 0$ бываютъ двоякаго рода: *первообразные* и *непервообразные*. Первообразными называются такіе, которые не удовлетворяютъ ни одному изъ уравненій

$$x - 1 = 0,\ x^2 - 1 = 0, \ldots x^{m-1} - 1 = 0.$$

Всякій непервообразный корень уравненія $x^m - 1 = 0$ есть первообразный корень другого уравненія $x^{m'} - 1 = 0$ степени ниже m, причемъ m' дѣлитъ m (n^0 127).

Теорема. *Число первообразныхъ корней уравненія $x^m - 1 = 0$ есть $\varphi(m)$. Всѣ они удовлетворяютъ уравненію*

$$\psi_m = \frac{\Pi(x^{m_1} - 1)}{\Pi(x^{m_2} - 1)} = 0.$$

На самомъ дѣлѣ, пусть f_m изображаетъ цѣлую функцію съ коэффиціентомъ у наивысшей степени перемѣннаго равнымъ единицѣ, корни которой суть первообразные корни уравненія $x^m = 1$; еслибы таковыхъ корней не существовало, то подъ f_m слѣдовало бы понимать единицу.

Изображая чрезъ $m, m', \ldots 1$ всѣ дѣлители числа m, мы замѣчаемъ, что каждый корень функціи $x^m - 1$ есть корень одной изъ функцій $f_m, f_{m'}, \ldots f_1$, и наоборотъ; а такъ какъ эти послѣднія общихъ корней очевидно имѣть не могутъ, то слѣдовательно имѣемъ равенство

$$f_m f_{m'} \ldots f_1 = x^m - 1,$$

которое вполнѣ опредѣляетъ собой функцію f_m. Изъ него выводимъ

$$f_m = \frac{\Pi(x^{m_1} - 1)}{\Pi(x^{m_2} - 1)},$$

то есть

$$f_m = \psi_m,$$

что и требовалось доказать.

142. Если a есть первообразный корень уравненія $x^m - 1 = 0$, то всѣ корни послѣдняго могутъ быть представлены такъ:

(1) . . . . $1,\ a,\ a^2,\ \ldots\ a^{m-1}$;

ибо всѣ числа (1) удовлетворяютъ ему очевидно, и всѣ они различны.

На самомъ дѣлѣ, допустивъ

$$a^i = a^{i'}, \quad (m > i > i'),$$

отсюда выводимъ

$$a^{i-i'} = 1,$$

что невозможно по причинѣ, что $i - i' < m$.

Возьмемъ теперь во вниманіе степень a^i, и обозначимъ чрезъ μ возможно малое положительное число, при которомъ удовлетворяется условіе

(2). . . . . $a^{\mu i} = 1$.

Такъ какъ по предположенію m есть самый малый показатель, при которомъ уравненіе $a^m = 1$ имѣетъ мѣсто, то для существованія уравненія (2) необходимо и достаточно (n^0 127), чтобъ μi дѣлилось на m, или, другими словами, чтобъ μ дѣлилось на $\frac{m}{d}$, гдѣ d есть общій наибольшій дѣлитель чиселъ m и i. Слѣдовательно имѣемъ

$$\mu = \frac{m}{d}.$$

Это приводитъ къ такой теоремѣ.

Теорема. *Если a есть первообразный корень уравненія $x^m - 1 = 0$, то степень a^i есть первообразный корень уравненія $x^{\frac{m}{d}} - 1 = 0$, гдѣ d изображаетъ общій наибольшій дѣлитель чиселъ i и m.*

Слѣдствіе. *Изъ одного какого нибудь первообразнаго корня a получаются всѣ остальные, если возвышать a въ степени простыя съ m и $< m$.*

Послѣднее свойство первообразнаго корня прямо относится къ корнямъ уравненія $\psi_m = 0$; по одному его корню получаются всѣ остальные возвышеніемъ въ степени простыя съ m и $< m$.

143. Обозначимъ чрезъ $\pi(x)$ какую нибудь изъ неприводимыхъ функцій, дѣлящихъ ψ_m; если намъ удастся доказать, что $\pi(x) = \psi_m$, то тѣмъ самымъ будетъ доказано, что функція ψ_m неприводима.

Возьмемъ уравненіе

$$\pi(x) = 0,$$

и положивъ $y = x^p$, гдѣ p простое число, не дѣлящее m, составимъ уравненіе съ y

$$\theta(y) = 0.$$

Обѣ функціи $\pi(x)$ и $\theta(y)$ одинаковой степени, а коэффиціенты у наивысшей степени перемѣннаго въ ихъ выраженіяхъ равны единицѣ.

Не трудно доказать, что функція $\theta(y)$ неприводима.

Допустимъ противное; пусть

$$(1) \ldots\ldots\ldots\ldots \theta(y) = \theta_1(y)\,\theta_2(y).$$

Изображая чрезъ p' число, удовлетворяющее условію

$$pp' \equiv 1 \pmod{m},$$

имѣемъ

$$y^{p'} = x^{pp'} = x^{1+tm},$$

гдѣ t изображаетъ цѣлое число.

Но $x^{tm} = 1$; слѣдовательно

$$(2) \ldots\ldots\ldots\ldots\ldots x = y^{p'}.$$

Итакъ, мы видимъ, что величины x и y выражаются раціональнымъ образомъ, какъ вторая чрезъ первую, такъ и первая чрезъ вторую.

Преобразовывая посредствомъ подстановки (2) оба уравненія

$$\theta_1(y) = 0, \quad \theta_2(y) = 0,$$

получаемъ соотвѣтственно два новыхъ уравненія

$$(3) \ldots\ldots\ldots\ldots \pi_1(x) = 0, \quad \pi_2(x) = 0.$$

Корни уравненія $\pi(x) = 0$ удовлетворяютъ частью первому уравненію (3), частью второму; поэтому заключаемъ

$$\pi(x) = \pi_1(x)\,\pi_2(x).$$

Но такое равенство невозможно, потому что функція $\pi(x)$ неприводима; слѣдовательно и равенство (1) также невозможно, то-есть функція $\theta(y)$ неприводима.

Всѣ корни функціи $\theta(x)$ очевидно удовлетворяютъ уравненію $x^m = 1$; а такъ какъ функція $\theta(x)$, будучи неприводимой, не можетъ имѣть кратныхъ корней, то слѣдовательно $x^m - 1$ дѣлится безъ остатка на $\theta(x)$.

Если теперь допустить, что функціи $\pi(x)$ и $\theta(x)$ различны, то тогда онѣ, будучи неприводимыми, будутъ взаимно простыми, и функція $x^m - 1$, дѣлясь на каждую порознь, раздѣлится на ихъ произведеніе.

Полагая

$$x^m - 1 = \pi(x)\,\theta(x)\,\lambda(x),$$

и замѣчая, что по теоремѣ Шенемана имѣемъ $\theta(x) \equiv \pi(x)$ (mod. p), заключаемъ

$$x^m - 1 \equiv \pi(x)^2\,\lambda(x) \pmod{p}.$$

Но это невозможно, ибо функція $x^m - 1$ по модулю p не имѣетъ двукратныхъ множителей; слѣдовательно первоначальное наше предположеніе ошибочно: функціи $\pi(x)$ и $\theta(x)$ тожественны.

Отсюда слѣдуетъ, что если x удовлетворяетъ уравненію $\pi(x)=0$, то всякая степень x^p, при p простомъ, не дѣлящемъ m, удовлетворяетъ также тому же уравненію.

Примѣняя послѣднее предложеніе нѣсколько разъ, мы приходимъ къ заключенію, что и степень x^n, при всякомъ n, простомъ съ m, будетъ удовлетворять уравненію $\pi(x)=0$.

Слѣдовательно, всѣ корни уравненія $\psi_m=0$ удовлетворяютъ уравненію $\pi(x)=0$.

Отсюда вытекаетъ равенство $\pi(x)=\psi_m$, что и требовалось доказать.

§ IV. Новое доказательство неприводимости функціи ψ_m при m равномъ степени простаго числа.

144. Въ частномъ случаѣ, когда m есть степень простаго числа, неприводимость функціи ψ_m доказывается легко съ помощью слѣдующей леммы.

Лемма. Каково бы ни было простое число p, функція вида

$$x^n+pa_1x^{n-1}+pa_2x^{n-2}+\ldots+pa_{n-1}x\pm p,$$

при цѣлыхъ значеніяхъ $a_1, a_2, \ldots a_{n-1}$, есть неприводимая.

Дѣйствительно, обозначимъ для сокращенія данную функцію чрезъ $f(x)$, и допустимъ, что она разлагается на произведеніе двухъ множителей

$$(1)\quad f(x)=(x^r+b_1x^{r-1}+\ldots+b_r)\,(x^s+c_1x^{s-1}+\ldots+c_s).$$

Приравнивая постоянные члены въ обѣихъ частяхъ (1), получаемъ уравненіе

$$b_r\,c_s=\pm p,$$

на основаніи котораго заключаемъ, что одинъ изъ членовъ b_r, c_s равенъ $\pm p$, остальной ∓ 1.

Положимъ

$$b_r=\pm 1,\quad c_s=\mp p;$$

вслѣдствіе этого изъ (1) вытекаетъ сравненіе

$$(2)\quad x^n \equiv (x^r + b_1 x^{r-1} + \ldots + b_{r-1} x \pm 1)(x^s + c_1 x^{s-1} + \ldots + c_{s-1} x) \pmod{p};$$

отсюда заключаемъ

$$c_{s-1} \equiv 0 \pmod{p}.$$

Вслѣдствіе этого сравненіе (2) можно написать проще такъ:

$$(3)\quad x^n \equiv (x^r + b_1 x^{r-1} + \ldots + b_{r-1} x \pm 1)(x^s + c_1 x^{s-1} + \ldots + c_{s-2} x^2) \pmod{p}.$$

Сравнивая въ обѣихъ частяхъ коеффиціенты у x^2, выводимъ

$$c_{s-2} \equiv 0 \pmod{p},$$

вслѣдствіе чего сравненіе (3) можно написать такъ:

$$(4)\quad x^n \equiv (x^r + b_1 x^{r-1} + \ldots + b_{r-1} x \pm 1)(x^s + c_1 x^{s-1} + \ldots + c_{s-3} x^3) \pmod{p}.$$

Продолжая разсуждать подобнымъ образомъ далѣе, въ концѣ дойдемъ до сравненія

$$x^n \equiv (x^r + b_1 x^{r-1} + \ldots + b_{r-1} x \pm 1) x^s \pmod{p}.$$

Сравнивая здѣсь коеффиціенты у x^s въ обѣихъ частяхъ, получаемъ невозможное сравненіе

$$1 \equiv 0 \pmod{p}.$$

Это показываетъ, что сравненіе (1) невозможно, то есть функція $f(x)$ неприводима.

145. Возьмемъ теперь во вниманіе функцію

$$\psi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1,$$

гдѣ p число простое.

ВcaptureНося $t+1$ на мѣсто x, получаемъ новую функцію

$$\psi_p(t+1)=(t+1)^p-1=t^p+\frac{p}{1}t^{p-1}+\ldots+p,$$

которая по виду своему очевидно подходитъ подъ предыдущую лемму; поэтому функція $\psi_p(t+1)$ неприводима.

Тѣмъ самымъ неприводима и первоначальная функція ψ_p.

146. Перейдемъ теперь къ болѣе общему случаю $m=p^\alpha$.

Внося въ выраженіи

$$(1)\quad \psi_{p^\alpha}=\frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1}=x^{p^{\alpha-1}(p-1)}+x^{p^{\alpha-1}(p-2)}+\ldots+1$$

$t+1$ на мѣсто x, получаемъ новую функцію

$$(2)\ \ldots\ \psi_{p^\alpha}(t+1)=\frac{(t+1)^{p^\alpha}-1}{(t+1)^{p^{\alpha-1}}-1}$$

$$=t^{p^{\alpha-1}(p-1)}+at^{p^{\alpha-1}(p-1)-1}+\ldots+k.$$

Чтобы получить значеніе k дѣлаемъ въ послѣднемъ равенствѣ $t=0$; находимъ

$$(3)\quad k=\psi_{p^\alpha}(1)=1^{p^{\alpha-1}(p-1)}+1^{p^{\alpha-1}(p-2)}+\ldots+1=p.$$

Далѣе, мы замѣчаемъ два тожественныя сравненія

$$\left.\begin{aligned}(t+1)^{p^\alpha}-1&\equiv t^{p^\alpha}\\(t+1)^{p^{\alpha-1}}-1&\equiv t^{p^{\alpha-1}}\end{aligned}\right\}\ (\text{mod. } p).$$

Отсюда слѣдуетъ, что частное отъ дѣленія по модулю p функціи $(t+1)^{p^\alpha}-1$ на функцію $(t+1)^{p^{\alpha-1}}-1$ сравнимо съ частнымъ отъ дѣленія функціи t^{p^α} на функцію $t^{p^{\alpha-1}}$, то есть

$$(4)\ \ldots\ldots\ \psi_{p^\alpha}(t+1)\equiv t^{p^{\alpha-1}(p-1)}\ (\text{mod. } p).$$

Изъ (2) и (4) выводимъ

$$t^{p^{\alpha-1}(p-1)}\equiv t^{p^{\alpha-1}(p-1)}+at^{p^{\alpha-1}(p-1)-1}+\ldots+k\ (\text{mod. } p),$$

откуда заключаемъ, что всѣ коеффиціенты $a, b, \ldots k$ входящіе во вторую часть (2) дѣлятся на p.

Принимая это въ соображеніе и замѣчая, что значеніе постояннаго члена k равно p, мы заключаемъ, что функція (2) подходитъ подъ вышедоказанную лемму; поэтому она неприводима. Отсюда слѣдуетъ, что и функція (1) неприводима.

147. Если какая нибудь функція $f(x)$ окажется неприводимою по модулю p, то подавно она абсолютно неприводима. Однако нельзя утверждать обратно; бываютъ функціи абсолютно неприводимыя, которыя разлагаются на множители относительно всякаго простаго модуля.

Такой интересный случай представляетъ функція ψ_m, когда число m не имѣетъ первообразныхъ корней.

Для примѣра возьмемъ неприводимую функцію

$$\psi_8 = x^4 + 1,$$

и постараемся доказать прямымъ путемъ, что эта функція приводима по всякому модулю.

Разсмотримъ отдѣльно четыре случая.

Первый случай, модуль $p = 2$. Тогда имѣемъ очевидно

$$x^4 + 1 \equiv (x + 1)^4 \pmod{2},$$

и слѣдовательно разсматриваемая функція приводима.

Второй случай, $p = 4n + 1$. Тогда сравненіе

$$x^2 + 1 \equiv 0 \pmod{p}$$

возможно. Обозначая чрезъ a одно изъ его рѣшеній, имѣемъ

$$x^4 + 1 \equiv (x^2 + a)(x^2 - a) \pmod{p}.$$

Это показываетъ, что функція $x^4 + 1$ приводима.

Третій случай, $p = 8n + 1$. Тогда сравненіе

$$x^2 \equiv 2 \pmod{p}$$

имѣетъ рѣшеніе. Обозначая его чрезъ a, имѣемъ

$$x^4 + 1 \equiv (x^2 + ax + 1)(x^2 - ax + 1) \pmod{p},$$

и слѣдовательно функція $x^4 + 1$ приводима.

Четвертый случай, $p = 8n - 1$. Сравненіе

$$x^2 + 2 \equiv 0 \pmod{p}$$

имѣетъ рѣшеніе, которое обозначимъ чрезъ a. Имѣемъ

$$x^4 + 1 \equiv (x^2 + ax - 1)(x^2 - ax - 1) \pmod{p};$$

слѣдовательно функція $x^4 + 1$ приводима.

Если теперь принять въ соображеніе, что всякое простое число p представляетъ непремѣнно одинъ изъ вышеразсмотрѣнныхъ четырехъ случаевъ, то становится ясно, что по какому бы то ни было модулю функція $x^4 + 1$ всегда приводима.

КОНЕЦЪ ВТОРОЙ ЧАСТИ.

53 005 ЕЯ L 4756

QA 155 .S65 1882 C.1
Vysshaia algebra /
Stanford University Libraries
3 6105 034 783 907

DATE DUE			

STANFORD UNIVERSITY LIBRARIES
STANFORD, CALIFORNIA 94305



